ViPNet SafeDisk 3.3

Benutzerhandbuch

ViPNet
Virtual Private Network
infotecs

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Copyright

1991–2014 Infotecs GmbH, Berlin

Version: 00012-06 34 01 DEU

Dieses Dokument ist Teil des Softwarepaketes und unterliegt daher denselben Lizenzbestimmungen wie das Softwareprodukt.

Dieses Dokument oder Teile davon dürfen nicht ohne die vorherige schriftliche Zustimmung der Infotecs GmbH verändert, kopiert, weitergegeben etc. werden.

ViPNet ist ein registriertes Warenzeichen des Softwareherstellers Infotecs GmbH.

Marken

Alle genannten Markennamen sind Eigentum der jeweiligen Hersteller.

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.biz

Inhalt

Einführung 8
Über dieses Dokument 9
Zielgruppe 9
Verwendete Konventionen 9
Über dieses Programm 11
Neu in Version 3.3.0 12
Systemanforderungen 15
Einschränkungen der kostenlosen Version 16
Lieferumfang 17
Kontakt 18
FAQ und andere Hilfsinformation 18
Kontakt 18

Kapitel 1. Allgemeines 19
Einsatzmöglichkeiten von ViPNet SafeDisk 20
Die Prinzipen des ViPNet SafeDisk Datenschutzes. Ein Überblick 21

Kapitel 2. ViPNet SafeDisk installieren, starten, aktualisieren und deinstallieren 22
ViPNet SafeDisk installieren 23
ViPNet SafeDisk aktualisieren 24
Konvertierung des Containers 26
ViPNet SafeDisk starten 29
ViPNet SafeDisk beenden 30
Deinstallation von ViPNet SafeDisk 33

Kapitel 3. Arbeit mit ViPNet SafeDisk beginnen 35
ViPNet SafeDisk zum ersten Mal starten 36
Benutzerpasswort definieren 37
Eigenes Passwort definieren 37
Zufälliges Passwort generieren 38
Eigenschaften des zufälligen Passwortes ändern 39
Benutzerpasswort ändern 40

Kapitel 4. Registrierung von ViPNet SafeDisk 41
Vor der Registrierung von ViPNet SafeDisk 42
Warum ViPNet SafeDisk registriert werden sollte 42
Registrierung starten 42
Seriennummer anfordern 44
Registrierungscode anfordern 45
Registrierungsanfrage über das Internet 45
Registrierungsanfrage via E-Mail 48
Registrierungsanfrage per Telefon 50
Registrierungsanfrage per Registrierungsdatei 51
ViPNet SafeDisk registrieren 54
Registrierungsdaten speichern 55
Wenn sich die Konfiguration Ihres Rechners geändert hat 56
Vorgehensweise bei der Registrierung per Registrierungsdatei 57

Kapitel 5. Datenschutz mit Hilfe von ViPNet SafeDisk 58
Vorgehensweise beim Datenschutz 60
Container erstellen 61
Sicherungskopie der Container-Schlüssel 69
Assistenten zur Erstellung von Sicherungskopien der Containerschlüssel starten 70
Sicherungskopie der Containerschlüssel erstellen 70
Container einbinden 74
Container einbinden, der durch eine Schlüssel-Datei geschützt ist 76
Container einbinden, der durch eine Authentisierungsgeräti geschützt ist 77
Einen früher erstellen Container einbinden 77
Container formatieren 79
Tägliche Arbeit mit den geschützten Daten 81
Containersymbole in ViPNet SafeDisk 82
Container trennen 83
Containereigenschaften ansehen und ändern 85
Containerschlüssel aktualisieren 88
Container-Datei verschieben 90
Container löschen 91
Parameter von ViPNet SafeDisk einstellen 92

Kapitel 6. Geschützte Daten exportieren und importieren 94

Zweck des Exports und Imports geschützter Daten 95
Container exportieren 97
Container auf den Rechner importieren 100
Container aus einer Export-Datei importieren 100
Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren 103
Sicherungskopie der Containerschlüssel auswählen 107

Kapitel 7. Wiederherstellen des Zugriffs auf die geschützten Daten 108
Warum Daten wiederhergestellt werden müssen 109
Lösungsvorschläge für die Wiederherstellung geschützter Daten 110
Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen 112
Sicherungskopie der Konfiguration erstellen 112
Liste von Sicherungskopien der Konfiguration editieren 114
Konfiguration wiederherstellen 115
Letzte Wiederherstellung der Konfiguration rückgängig machen 117

Kapitel 8. Gemeinsame Nutzung von ViPNet SafeDisk 118
Zugriff auf die geschützten Daten verwalten. Neuen Benutzer registrieren 119
Zugriff auf die Container für mehrere Benutzer einrichten 121
Abgrenzung des Containerzugangs 122
Containerzugang für einen oder mehrere Benutzer auf demselben oder auf unterschiedlichen Computern bereitstellen 123
Netzwerkzugang auf einen Container für mehrere Benutzer ermöglichen 124
Netzwerkzugang auf einen Container für die anderen Benutzer deaktivieren 129
Auf dem Server gespeicherte Daten schützen 130
Vertrauliche Daten mit Hilfe eines Kuriers oder über das Netzwerk übertragen 132

Kapitel 9. Arbeit in einer potentiell unsicheren Umgebung 133
Vorbereitung für den Einsatz in einer unsicheren Umgebung: Vorgehensweise 134
Arbeit unter Kontrolle der Attentäter 135
Vorbereitung auf die Arbeit unter Kontrolle der Attentäter 135
Arbeit unter Kontrolle der Attentäter 135
Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus 136
Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus 139
Tastenkombinationen (Hotkeys) für den „Gefahr“ und „Extreme Gefahr“ Modus 142

Kapitel 10. Spurenbeseitigung bei der Arbeit mit privaten Daten 143

Warum die Datenbereinigung notwendig ist 144
Vorgehensweise beim Bereinigen von Datenspuren 146
Bereinigung von Datenspuren: Reihenfolge der Schritte 148
Datenspuren in Windows bereinigen 149
Liste zuletzt verwendeter Dateien löschen 149
Temporäre Dateien löschen 149
Papierkorb bereinigen 150
Sicheres Löschen ungeschützter Dateien 150
Dateien sicher löschen 151
Freien Speicherplatz auf Laufwerken bereinigen 151
Laufwerke für standardmäßige Bereinigung des freien Speicherplatzes einstellen 152
Datenspuren im Internet Explorer bereinigen 154
Browserverlauf leeren 154
Temporäre Internetdateien löschen 154
Cookies bereinigen 155
Vollständige Bereinigung 157
Vollständige Bereinigung einstellen 159
Bereinigung über die Befehlszeile starten 160

Kapitel 11. Suche und Beseitigung von Störungen 162
Logdatei ansehen 163
Typische Problemfälle 164
Container ist nicht verfügbar 164
Laufwerk kann nicht formatiert werden 164
Container-Datei wurde nicht gefunden 164
Verbindung zum Container ging verloren 165
Container kann nicht eingebunden werden 165
Das Komprimierungs- oder das Verschlüsselungsattribut der Container-Datei ist gesetzt 166
Container mit Zugriffstyp „Authentisierungsgerät“ konnte nicht erstellt werden 167

Anhang A. Versionsgeschichte 168
Version 3.2.2 168
Version 3.2.1 168
Version 3.2.0 169
Version 3.1.1 169

Version 3.1.0 169

Anhang B. Externe Datenträger 171

Anhang C. Regionaleinstellungen 173

Anhang D. 179

Anhang E 182

Einführung

Über dieses Dokument	9
Über dieses Programm	11
Neu in Version 3.3.0	12
Systemanforderungen	15
Einschränkungen der kostenlosen Version	16
Lieferumfang	17
Kontakt	18

Über dieses Dokument

Zielgruppe

Dieses Handbuch ist für alle bestimmt, die das Programm ViPNet SafeDisk für den schnellen, einfachen und effektiven Schutz von Daten einsetzen wollen.

Zu Beginn des Handbuchs werden die allgemeinen Grundlagen der Technologie von ViPNet SafeDisk erklärt. Anschließend wird der Vorgang der die Installation und Registrierung von ViPNet SafeDisk beschrieben. In den nachfolgenden Kapiteln erfahren Sie mehr über die Aufgaben, die mit Hilfe von ViPNet SafeDisk gelöst werden können. Am Ende wird eine kurze Übersicht von Anleitungen zur Suche und Beseitigung von Störungen geboten, womit einige häufig auftretende Probleme schnell beseitigt werden können.

Das in diesem Handbuch vorgestellte Material ist nach steigendem Schwierigkeitsgrad angeordnet. Nach dem Erhalt der notwendigen Informationen können Sie mit dem Lesen aufhören und zum Handbuch wieder zurückkehren, wenn dazu die Notwendigkeit besteht.

Die Kapitel können auch in beliebiger Reihenfolge gelesen werden. Sie finden die benötigten Informationen bequem mit Hilfe der Inhaltsübersicht und des Stichwortverzeichnisses.

Beim Verfassen dieses Handbuchs sind wir davon ausgegangen, dass der Leser über Basiskenntnisse über das Betriebssystem Windows verfügt und sich über die Notwendigkeit des Schutzes vertraulicher Daten im Klaren ist.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	Achtung! Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	Hinweis. Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.

Symbol	Beschreibung
	Tipp. Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.
Menü > **Untermenü** > **Befehl**	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsbereich.
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Über dieses Programm

In den letzten Jahren gewann die Information in elektronischer Form zunehmend an Wert. Die Folgen des Verlustes vertraulicher Daten wurden immer schwerwiegender.

Die Angreifer oder nicht berechtigte Personen können Interesse haben sich Zugang zu den Geschäftsbriefen, Firmenberichten, Forschungsergebnissen und anderen sensiblen Daten zu verschaffen. Dies kann zum materiellen Schaden, Imageverlust oder Verlust des geistigen Eigentums führen.

Der Schutz sensibler Daten vom unberechtigten Lesen, Kopieren, Verändern und Löschen wird immer wichtiger. Zusätzliche Schutzmassnahmen sind insbesondere für Laptops empfehlenswert, da es leicht zum Verlust des Gerätes kommen kann. Gleichzeitig ist es notwendig, den berechtigten Personen, zum Beispiel den Mitarbeitern, den Zugang zu den Daten zu ermöglichen.

Die Anforderungen and die Sicherheitssoftware steigen ebenfalls. Die Schutzprogramme sollen benutzerfreundlich und selbst für die Benutzer mit geringen PC-Kenntnissen leicht bedienbar sein, die Ver- und Entschlüsselung soll automatisiert, aber transparent sein. Außerdem sollen sie in alle vorhandenen und gewöhnlichen Arbeitsprozesse integrierbar sein.

ViPNet SafeDisk entspricht allen diesen Anforderungen im höchsten Masse und bietet Ihren Daten einen sicheren Schutz von Unbefügten.

Neu in Version 3.3.0

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten von ViPNet SafeDisk der Version 3.3.0 geboten.

- **Zwangsweise Trennung des Containers**

  Es besteht die Möglichkeit zur zwangsweisen Trennung des Containers, wenn die im Container enthaltenen Dateien von anderen Anwendungen benutzt werden.

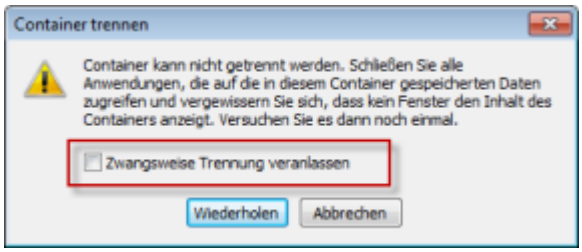
Container trennen
Container kann nicht getrennt werden. Schließen Sie alle Anwendungen, die auf die in diesem Container gespeicherten Daten zugreifen und vergewissern Sie sich, dass kein Fenster den Inhalt des Containers anzeigt. Versuchen Sie es dann noch einmal.
Zwangsweise Trennung veranlassen
Wiederholen
Abbrechen

Abbildung 1: Zwangsweise Trennung des Containers

- **Austausch von Containerschlüsseln**

  Damit die Sicherheit beim Schutz von Daten, die in Containern gespeichert sind, erhöht werden kann, besteht die Möglichkeit zum Aktualisieren der Containerschlüssel, mit denen der Containerinhalt verschlüsselt wurde. Nach der Aktualisierung wird der Zugang zum Container unter Verwendung alter Schlüssel nicht mehr möglich sein. Es wird empfohlen, die Aktualisierung der Containerschlüssel nicht seltener als alle 15 Monate durchzuführen.

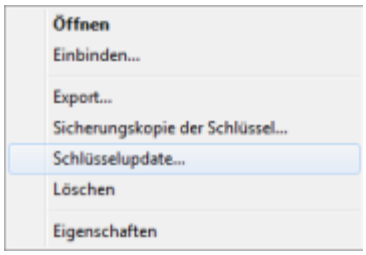

Abbildung 2: Containerschlüsselupdate

- **Speicherung der Sicherungskopie der Containerschlüssel auf einem externen Gerät**

  Damit die Sicherheit beim Schutz von Daten, die in Containern gespeichert sind, erhöht werden kann, besteht nun die Möglichkeit zum Speichern von Sicherungskopien der Containerschlüssel auf einem externen Gerät (Authentisierungsgerät). Details s. Liste unterstützter Geräte (s. Externe Datenträger auf Seite 171).

- **Formatierung des Containers**

  Zum Formatieren des Containers wurde früher die Standardschnittstelle von Microsoft Windows verwendet. Aus praktischen Gründen wurde dafür nun ein Assistent zur Containerformatierung implementiert. Der Assistent zur Containerformatierung wird beim Einbinden eines nicht formatierten Containers automatisch gestartet.

Container formatieren
Container formatieren
Damit der Container benutzt werden kann, muss er formatiert werden. Dieser Vorgang kann einige Minuten in Anspruch nehmen.
Container: Container32CB
Dateisystem: NTFS
Klicken Sie auf "Weiter", um die Formatierung zu starten. Der Vorgang der Formatierung kann später nicht mehr unterbrochen werden.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 3: Eine Möglichkeit den Container mit Hilfe des Assistenten zu formatierem

- **Änderung in den Einschränkungen der kostenlosen Version**

  In der kostenlosen Programmversion war die maximale Größe des Containers zuvor auf 100 MB beschränkt. Nun beträgt die maximale Containergröße der kostenlosen Version 1 GB.

- **Erweiterung der Größe des standardmäßig angelegten Containers**

  Zuvor betrug die Standardgröße eines Containers 100 KB. Aus praktischen Gründen und um den geänderten Anforderungen im Hinblick auf den Datenumfang zu entsprechen, beträgt die Größe des standardmäßig angelegten Containers nun 100 MB.

- **Gleichzeitige, unabhängige Verwendung des Programms ViPNet SafeDisk in unterschiedlichen Sitzungen des Betriebssystems**

  Mehrere Instanzen des Programms können nun gleichzeitig und unabhängig voneinander in unterschiedlichen Sitzungen des Betriebssystems ausgeführt werden. Diese Funktionalität erlaubt es den Benutzern, auf ein und demselben Computer gleichzeitig und unabhängig voneinander mit dem Programm zu arbeiten. Jeder Benutzer arbeitet dabei in seiner eigenen Sitzung des Betriebssystems.

- **Exklusiver Zugriff**

Nun kann der Containerzugang in den Betriebssystemen Microsoft Windows XP SP3 (32-Bit)/Server 2003 (32/64-Bit) eingeschränkt werden, indem beim Einbinden des Containers das Kontrollkästchen Exklusiver Zugriff aktiviert wird. Früher konnte der Containerzugang ausschließlich mit Mitteln des Betriebssystems eingeschränkt werden.

Abbildung 4: Exklusiver Zugriff

- **Keine Notwendigkeit zum Neustart des Computers bei Programmupdates**

  Zuvor wurde bei Aktualisierungen des Programms ViPNet SafeDisk ein Neustart des Computers benötigt, um Änderungen wirksam zu machen. Nun ist ein Neustart nicht mehr erforderlich.

- **Verbesserung der Dokumentation und Hilfe**

  Dokumentation und Hilfe wurden überarbeitet. Beschreibungen neuer Programmfunktionen wurden hinzugefügt; Informationen betreffend die Änderungen in der Schnittstelle wurden aktualisiert.

Systemanforderungen

Zur erfolgreichen Arbeit mit ViPNet SafeDisk soll Ihr PC folgenden minimalen Anforderungen entsprechen:

- Prozessor: Intel Core 2 Duo oder andere x86-kompatibel Prozessor mit zwei Kernen oder mehr ist empfohlen.
- Mindestens 128 MB RAM.
- Mindestens 20 MB freier Speicherplatz.
- Betriebssysteme: Windows XP SP3 (32 Bit)/Server 2003 (32/64 Bit)/ Vista SP2 (32/64 Bit)/Server 2008 (32/64 Bit)/Windows 7 (32/64 Bit).
- Internet Explorer 6.0 oder höher.

ViPNet SafeDisk unterstützt Authentiserungstechnologien. Mehr über die Arbeit mit Authentisierungsgeräten lesen Sie in der Anleitung Externe Datenträger (auf Seite 171).

Einschränkungen der kostenlosen Version

Beginnend mit der Version 3.1 besteht nun die Möglichkeit, mit einer kostenlosen Version von ViPNet SafeDisk zu arbeiten. Die Nutzungsdauer der kostenlosen Version ist nicht begrenzt, es gibt jedoch einige funktionelle Einschränkungen.

In einer nicht registrierten Version von ViPNet SafeDisk 3.3 gelten folgende funktionelle Einschränkungen:

- Anzahl der Benutzer: maximal 1.
- Anzahl der Container: maximal 1.
- Containergröße: maximal 1 GB.

Die aufgeführten Einschränkungen können durch eine Registrierung des Programms (s. Registrierung von ViPNet SafeDisk auf Seite 41). aufgehoben werden. Um zu erfahren, ob Ihre Programmversion von ViPNet SafeDisk registriert ist, wählen Sie im Menü **Hilfe** den Befehl **Über ViPNet SafeDisk**.

Falls das Programm ViPNet SafeDisk 3.3 oder höher über die registrierte Version 2.9 oder niedriger installiert wird, sind folgende funktionelle Einschränkungen zu beachten: alle Benutzer, die vormals im Programm der Version 2.9 registriert wurden, haben die Möglichkeit, mit bestehenden Containern und Sicherungskopien zur Wiederherstellung der Konfiguration weiter zu arbeiten. Zum Erstellen oder Importieren neuer Container und zum Registrieren neuer Benutzer sollte das Programm jedoch neu registriert werden.

Falls das Programm ViPNet SafeDisk 3.3 oder höher über die registrierte Version 3.0, 3.1, 3.2 installiert wird, funktioniert die neue Version ohne Einschränkungen.

Falls das Programm ViPNet SafeDisk 3.3 oder höher über eine beliebige Demoversion (registriert oder innerhalb eines begrenzten Zeitraums gültig) installiert wird, gibt es keine Möglichkeit mehr, mit der bestehenden Konfiguration (mit Benutzerliste, mit Containern und Sicherungskopien zur Wiederherstellung der Konfiguration) weiter zu arbeiten, d. h. das Programm wird wie nach einer erstmaligen Installation mit Einschränkungen der kostenlosen Version arbeiten.

Lieferumfang

Zum Lieferumfang von ViPNet SafeDisk gehören:

- Installationsdatei ViPNet SafeDisk – Setup.exe;
- „ViPNet SafeDisk 3.3. Benutzerhandbuch“.

Die Dokumentation wird in elektronischer Form im Format PDF geliefert.

Kontakt

FAQ und andere Hilfsinformation

Informationen über ViPNet Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/agb.htm
- ViPNet Lösungen im Überblick http://www.infotecs.de/produkte.htm
- ViPNet Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Fachleuten der Firma „InfoTeCS“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail support@infotecs.biz
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support.htm
- Support Hotline +49 (0) 30 206 43 66 0 (Tel.); +49 (0) 30 206 43 66 66 (Fax).

1

Allgemeines

Einsatzmöglichkeiten von ViPNet SafeDisk 20

Die Prinzipen des ViPNet SafeDisk Datenschutzes. Ein Überblick 21

Einsatzmöglichkeiten von ViPNet SafeDisk

ViPNet SafeDisk hilft Ihnen dabei, folgende Aufgaben schnell und effektiv zu lösen:

- Sie wollen sicher sein, dass Ihre Verwandten, Freunde und Kollegen nicht die Möglichkeit haben, absichtlich oder durch Zufall, wichtige Dokumente einzusehen, zu ändern oder zu löschen;
- Sie speichern Daten auf einem Notebook und wollen nicht, dass diese von irgendjemandem sonst gelesen, kopiert oder benutzt werden (falls das Notebook verloren oder gestohlen wird);
- vertrauliche Daten werden auf mehreren Computern aufbewahrt (zum Beispiel zu Hause und im Büro) und Sie wollen die Rechner so schützen, dass ein sicherer Datenaustausch zwischen den Computern möglich wird;
- Sie wollen vertrauliche Daten mit Hilfe eines externen Datenträgers übertragen und gleichzeitig verhindern, dass die Daten verloren gehen oder gestohlen werden;
- Sie wollen den Zugang zu vertraulichen Daten auf einem oder mehreren Computern steuern können (zum Beispiel den Zugang zu Dokumenten für einige Benutzer erlauben und für andere Benutzer blockieren);
- bei der Annäherung Dritter wollen Sie den Zugang zu sensiblen Daten sperren und die Präsenz dieser Daten verbergen können;
- bei der Annäherung von Übeltätern wollen Sie alle vertraulichen Daten schnell und sicher löschen können.

Die Prinzipen des ViPNet SafeDisk Datenschutzes. Ein Überblick

In ViPNet SafeDisk werden die Daten in Containern gespeichert. Ein Container ist eine verschlüsselte Datei, die mit einem Passwort, einer Schlüsseldatei oder einem Authentisierungsgerät geschützt ist. Beim Erstellen des Containers wird sein Schutzmodus festgelegt: Passwort, Schlüssel-Datei oder Authentisierungsgerät.

Nach dem Einbinden wird der Container im System als ein gewöhnliches Laufwerk dargestellt, auf welchem vertrauliche Informationen abgelegt werden können.

Beim Speichern werden die Daten automatisch verschlüsselt und beim Auslesen automatisch entschlüsselt. Die Verschlüsselung erfolgt schnell und unauffällig, mit den Dokumenten kann wie im Normalbetrieb weitergearbeitet werden, die Daten werden dabei aber zuverlässig geschützt.

Die Ver- und Entschlüsselung der Daten erfolgt sektorweise beim Speichern und Lesen. Dementsprechend wird der Vorgang der Ver- oder Entschlüsselung nur für die Daten vollzogen, die zum aktuellen Zeitpunkt unmittelbar gebraucht werden. Das gewährleistet eine hohe Geschwindigkeit bei der Arbeit mit geschützten Daten und eine hohe Transparenz für die Benutzer der Anwendung.

Wenn sich der Container auf einem Netzlaufwerk befindet, werden die Daten verschlüsselt über das Netzwerk übertragen; die Ver- und Entschlüsselung erfolgt auf dem lokalen Rechner.

Nach dem Trennen wird der Container nicht mehr im System angezeigt. Die Präsenz vertraulicher Daten kann nicht mehr festgestellt werden, der Zugang zu diesen Daten ist nicht mehr möglich.

Zum Wiederherstellen des Zugangs zu den im Container abgelegten Daten und zum Fortsetzen der Arbeit mit diesen Daten muss der Container wieder eingebunden werden. Sie brauchen dafür ein Passwort, eine Schlüsseldatei oder ein Authentisierungsgerät je nach dem gewählten Zugriffstyp.

ViPNet SafeDisk installieren, starten, aktualisieren und deinstallieren

ViPNet SafeDisk installieren	23
ViPNet SafeDisk aktualisieren	24
ViPNet SafeDisk starten	29
ViPNet SafeDisk beenden	30
Deinstallation von ViPNet SafeDisk	33

ViPNet SafeDisk installieren

Achtung! Falls ViPNet SafeDisk auf einem Computer mit Windows-Betriebssystem installiert wird, das nicht über die deutsche Lokalisierung verfügt, können Probleme bei der Darstellung von Umlauten und „ß“ im Interface von ViPNet SafeDisk auftreten. Um dies zu vermeiden, ändern Sie bitte die Regionaleinstellungen des Windows-Betriebssystems (s. Regionaleinstellungen auf Seite 173).

Um ViPNet SafeDisk zu installieren, müssen Sie über Administratorrechte verfügen. Um ViPNet SafeDisk zu installieren, führen Sie die folgenden Schritte durch:

1. Starten Sie die Programminstallation (die Datei `setup.exe`), indem Sie doppelt auf das Symbol klicken. Der ViPNet SafeDisk Installations-Assistent wird gestartet.
2. Folgen Sie den Hinweisen des Installations-Assistenten.
3. Sie können ViPNet SafeDisk nach der Installation registrieren.

   Unregistrierte Free Edition von ViPNet SafeDisk ist kostenlos und kann zeitlich uneingeschränkt genutzt werden, sie hat aber einige funktionale Einschränkungen (s. Einschränkungen der kostenlosen Version auf Seite 16).

   Um ViPNet SafeDisk im vollen Umfang nutzen zu können muss das Programm registriert werden.

   Mehr über die Registrierung von ViPNet SafeDisk lesen Sie in ViPNet SafeDisk registrieren (s. Registrierung von ViPNet SafeDisk auf Seite 41).

ViPNet SafeDisk aktualisieren

Achtung! Eine Aktualisierung des Programms ViPNet SafeDisk sollte unbedingt in der weiter unten aufgeführten Reihenfolge vorgenommen werden.

Für das Upgrade des Programms ViPNet SafeDisk wird eine Installationsdatei der neuen Version der Software benötigt. Damit das Upgrade erfolgreich durchgeführt werden kann, gehen Sie folgendermaßen vor:

1 Vor Beginn des Upgrades sollten Sie in Abhängigkeit davon, welche Version zum gegenwärtigen Zeitpunkt installiert ist, die folgenden Schritte ausführen:

- Wenn die laufende Version von ViPNet SafeDisk 2.9 oder niedriger ist und beim Erstellen des Containers als Zugriffstyp **Authentisierungsgerät** ausgewählt wurde, dann sollte zunächst der Zugriffstyp zu diesen Containern geändert werden (s. Containereigenschaften ansehen und ändern auf Seite 85). Container, die unter Verwendung dieser Zugangsart erstellt wurden, können nicht in das neue Format, das von der Version 3.3 unterstützt wird, konvertiert werden.
- Wenn die laufende Versionnummer von ViPNet SafeDisk 3.0 oder 3.1 ist, dann erstellen Sie zunächst Sicherungskopien der Schlüssel von Containern mit der Zugriffstyp **Authentisierungsgerät**. Dies wird benötigt, um nach der Konvertierung der Container in das neue Format den Containerzugang wieder sicherzustellen.

Achtung! Wenn keine Sicherungskopien der Containerschlüssel erstellt werden, stehen Daten, die in diesen Containern gespeichert sind, nicht mehr zur Verfügung. Sie können den Zugang zu diesen Daten erhalten, indem Sie die vorhergehende Version von ViPNet SafeDisk installieren.

- Wenn die laufende Version 3.2 oder höher ist, sind keine zusätzlichen Schritte nötig.

Tipp. Zum Ermitteln der Programmversion, die bei Ihnen installiert ist, wählen Sie im Menü **Hilfe** den Eintrag **Über ViPNet SafeDisk**.

2 Erstellen Sie eine Sicherungskopie Ihrer Daten. Führen Sie dazu eine der folgenden Aktionen aus:

- Kopieren Sie die Containerdateien und die Sicherungskopien der Containerschlüssel an einen sicheren Ort.
- Erstellen Sie Exportdateien für alle Ihre Container und kopieren Sie diese an einen sicheren Ort.

3 Machen Sie sich mit den Besonderheiten einer Aktualisierung der laufenden Programmversion von ViPNet SafeDisk auf die Version 3.3 vertraut:

- Wenn die laufende Programmversion 2.9 oder niedriger ist, dann wird im Zuge eines Updates die neue, kostenlose Version ViPNet SafeDisk 3.3 installiert, die jedoch einigen Einschränkungen unterliegt. Zum Aufheben dieser Einschränkungen sollte die zu installierende Version von ViPNet SafeDisk neu gekauft und registriert werden.
- Wenn die laufende Version eine Demoversion ist, dann wird im Zuge eines Updates die neue, kostenlose Version ViPNet SafeDisk 3.3 installiert. Es wird keine Möglichkeit mehr geben, mit den zuvor erstellten Containern, Benutzern oder Sicherungskopien der Konfiguration zu arbeiten.
- Wenn die laufende Programmversion 3.2 oder niedriger ist, dann wird vom Programm eine Meldung über die Änderung des Containerformats mit dem Hinweis, bereits angelegte Container zu konvertieren, angezeigt.

  Alle Sicherungskopien der Konfiguration, die in den vorhergehenden Versionen von ViPNet SafeDisk (3.2 und niedriger) erstellt wurden, werden gelöscht.

4 Entladen Sie alle Komponenten der Software ViPNet SafeDisk aus dem Hauptspeicher des Computers.

5 Starten Sie durch einen Doppelklick das Installationsprogramm `setup.exe` . Es wird der Installationsassistent von ViPNet SafeDisk gestartet.

Wenn bei Ihnen zuvor Programmversion 3.2 oder niedriger installiert war und bereits Container erstellt wurden, dann wird der Assistent **ViPNet SafeDisk Update** gestartet.

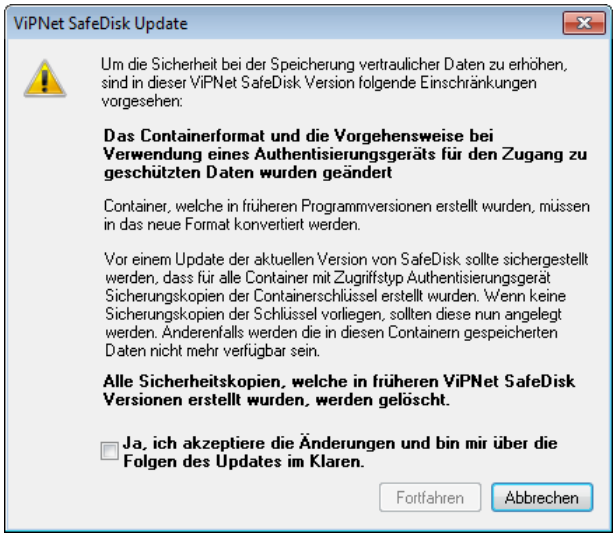
ViPNet SafeDisk Update
Um die Sicherheit bei der Speicherung vertraulicher Daten zu erhöhen, sind in dieser ViPNet SafeDisk Version folgende Einschränkungen vorgesehen:
Das Containerformat und die Vorgehensweise bei Verwendung eines Authentisierungsgeräts für den Zugang zu geschützten Daten wurden geändert
Container, welche in früheren Programmversionen erstellt wurden, müssen in das neue Format konvertiert werden.
Vor einem Update der aktuellen Version von SafeDisk sollte sichergestellt werden, dass für alle Container mit Zugriffstyp Authentisierungsgerät Sicherungskopien der Containerschlüssel erstellt wurden. Wenn keine Sicherungskopien der Schlüssel vorliegen, sollten diese nun angelegt werden. Anderenfalls werden die in diesen Containern gespeicherten Daten nicht mehr verfügbar sein.
Alle Sicherheitskopien, welche in früheren ViPNet SafeDisk Versionen erstellt wurden, werden gelöscht.
Ja, ich akzeptiere die Änderungen und bin mir über die Folgen des Updates im Klaren.
Fortfahren
Abbrechen

Abbildung 5: Upgrade der Version ViPNet SafeDisk 3.2 und niedriger

Aktivieren Sie im Assistentenfenster das Kontrollkästchen **Ja, ich akzeptiere die Änderungen und bin mir über die Folgen des Updates im Klaren**. Dadurch sollen Container, die in Version 3.2 oder niedriger angelegt wurden, in das neue Format konvertiert und für den Einsatz in ViPNet SafeDisk 3.3 zur Verfügung gestellt werden. Damit Container in Version 3.3 eingebunden werden können, sollten sie umkonvertiert werden (s. Konvertierung des Containers auf Seite 26).

6 Warten Sie, bis der Assistent seine Arbeit abgeschlossen hat.

Wenn alle beschriebenen Schritte ordnungsgemäß durchgeführt wurden, verläuft die Aktualisierung erfolgreich und Sie können beginnen, mit dem Programm zu arbeiten.

Konvertierung des Containers

Zur Erhöhung der Sicherheit bei der Speicherung vertraulicher Daten wurde im Programm ViPNet SafeDisk Version 3.3 das Containerformat geändert. Container, die in früheren Versionen erstellt wurden, sollten in das neue Format konvertiert werden.

Zum Konvertieren der Container in das neue Format:

1 Starten Sie das Programm (s. ViPNet SafeDisk starten auf Seite 29).

2 Verbinden Sie den Container (s. Container einbinden auf Seite 74), der in einer früheren Version erstellt wurde. In Spalte **Status** wird bei diesem Container der Wert **Altes Format** angezeigt.

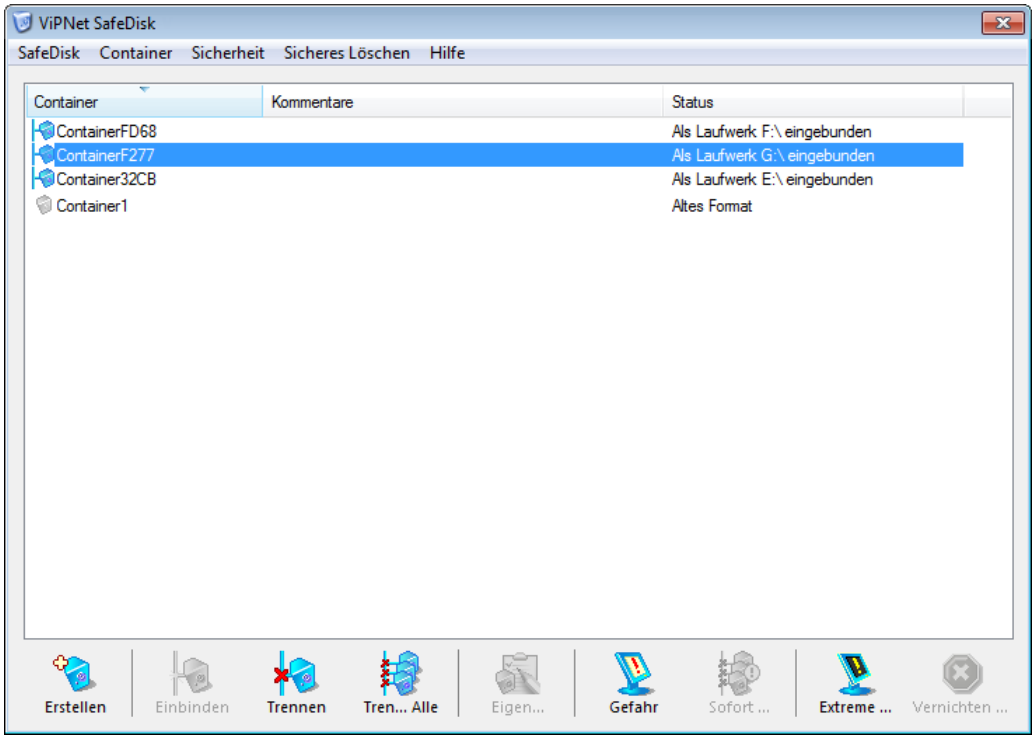

Abbildung 6: Verbindung des Containers, der in der früheren Version von ViPNet SafeDisk erstellt wurde

3 Dadurch wird ein Assistent zur Konvertierung des Containers gestartet.

Container konvertieren
Container konvertieren
Dieser Container wurde in einer früheren Version von ViPNet SafeDisk erstellt. Um den Container weiter verwenden zu können, muss er konvertiert werden.
Achtung! Um diesen Container in einer früheren Version von ViPNet SafeDisk weiter verwenden zu können, muss der Container vor der Konvertierung im alten Format exportiert werden.
Container im alten Format exportieren
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 7: Container in das neue Format konvertieren

Wenn Sie vor dem Programmupdate keinen Export des Containers im alten Format durchgeführt haben, dann aktivieren Sie im Fenster **Container konvertieren** das

Kontrollkästchen **Container im alten Format exportieren**. Dadurch wird der Assistent **Container-Export** gestartet. Führen Sie alle Schritte des Assistenten durch.

Tipp. Der Containerexport ist erforderlich, damit Sie die Möglichkeit haben, mit diesem Container bei einer Rückkehr zur früheren Version von ViPNet SafeDisk zu arbeiten. Deswegen empfehlen wir ausdrücklich, vor Beginn der Konvertierung einen Containerexport durchzuführen.

4 Warten Sie, bis der Konvertierungsprozess abgeschlossen ist.

Der Container wird nun in das neue Format konvertiert und kann anschließend in ViPNet SafeDisk Version 3.3 verwendet werden.

ViPNet SafeDisk starten

Zum Starten von ViPNet SafeDisk:

1 Führen Sie eine der Aktionen aus:

- Wählen Sie **Alle Programme** im Menü **Start** aus, dann **ViPNet**, danach **ViPNet SafeDisk** und klicken Sie auf **ViPNet SafeDisk** (im Zuge der Installation könnte sich die Position des Programmeintrags im Menü Start auch geändert haben)

- Doppelklicken Sie auf dem Desktop auf die Verknüpfung (die Verknüpfung wird auf dem Desktop angezeigt, wenn im Zuge der Programminstallation eine entsprechende Option gewählt wurde).

Das Passworteingabefenster öffnet sich. Wenn Sie ViPNet SafeDisk zum ersten Mal starten, folgen Sie den Anweisungen aus dem Abschnitt ViPNet SafeDisk zum ersten Mal starten (auf Seite 36).

Abbildung 8: Passworteingabefenster

2 Geben Sie das Passwort ein und klicken Sie auf **OK**. Das Hauptfenster von ViPNet SafeDisk öffnet sich.

Wenn Sie noch kein Passwort haben, klicken Sie auf den Link **das Passwort für den neuen Benutzer erstellen** und folgen Sie den Anweisungen (s. Zugriff auf die geschützten Daten verwalten. Neuen Benutzer registrieren auf Seite 119).

ViPNet SafeDisk beenden

Nachdem ViPNet SafeDisk alle erforderlichen Vorgänge abgeschlossen hat, können Sie:

- Das Programmfenster minimieren. Dabei bleibt das Programm aktiv, die Container bleiben verfügbar, das Hauptfenster wird aber in die Taskleiste minimiert. Wenn nötig, kann das Programmfenster wieder maximiert werden.
- Das Programm beenden. Dabei werden alle eingebundenen Container getrennt und die Arbeit des Programms wird beendet.

Führen Sie einen der folgenden Schritte aus, um das Programmfenster zu schließen:

- Klicken Sie auf die Schaltfläche im oberen rechten Teil des Fensters.
- Drücken Sie die Tastenkombination **Alt+F4**.

  Beim Versuch, das Programm zu schließen, wird das Fenster **Schließen des Fensters ViPNet SafeDisk** eingeblendet, in welchem Sie eine der zwei Aktionen ausführen können: Hauptfenster ausblenden oder Programm beenden. Wählen Sie die Option **Das Hauptfenster ausblenden, ohne dabei SafeDisk zu beenden** und klicken Sie auf **OK**.

Hinweis. Damit beim Klicken auf die Schaltfläche die gewählte Aktion ohne weitere Rückfragen durchgeführt wird, aktivieren Sie das Kontrollkästchen Dieses Fenster nicht mehr anzeigen. Die vorzunehmende Aktion beim Schließen des Fensters kann in den Programmeinstellungen konfiguriert werden (s. Parameter von ViPNet SafeDisk einstellen auf Seite 92).

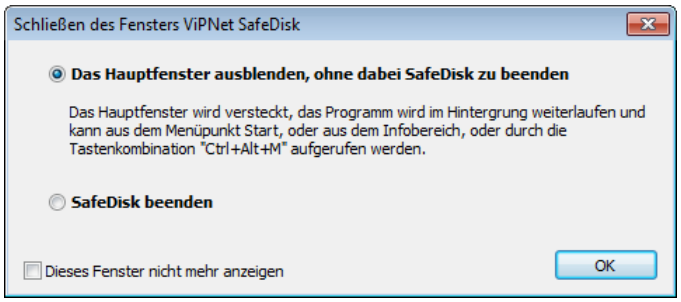
Schließen des Fensters ViPNet SafeDisk
Das Hauptfenster ausblenden, ohne dabei SafeDisk zu beenden
Das Hauptfenster wird versteckt, das Programm wird im Hintergrung weiterlaufen und kann aus dem Menüpunkt Start, oder aus dem Infobereich, oder durch die Tastenkombination "Ctrl+Alt+M" aufgerufen werden.
SafeDisk beenden
Dieses Fenster nicht mehr anzeigen
OK

Abbildung 9: Schließen des Fensters ViPNet SafeDisk

Tipp. Wenn Sie vorhaben, den Rechner für einige Zeit unbeaufsichtigt laufen zu lassen, empfiehlt es sich, die Option **SafeDisk beenden** auszuwählen.

Außerdem können Sie das Programm so einstellen, dass Container, mit denen aktuell nicht gearbeitet wird, automatisch getrennt werden. Dazu wählen Sie im Menü **SafeDisk** den Befehl **Einstellungen**. Aktivieren Sie im Fenster **Einstellungen** in Registerkarte **Allgemein** das Kontrollkästchen **Container trennen bei Inaktivität länger als**. Details s. Kapitel Parameter von ViPNet SafeDisk einstellen.

Führen Sie eine der folgenden Aktionen aus, um das Programmfenster wieder einzublenden:

- Klicken Sie im Infobereich der Taskleiste auf das Symbol .
- Drücken Sie die Tastenkombination **Strg+Alt+M**.
- Doppelklicken Sie auf dem Desktop die Verknüpfung .

Führen Sie einen der folgenden Schritte aus, um das Programm ViPNet SafeDisk zu beenden:

- Klicken Sie im Infobereich der Taskleiste mit der rechten Maustaste auf das Symbol und wählen Sie den Befehl **Beenden**.
- Wählen Sie im Hauptfenster im Menü **SafeDisk** den Befehl **Beenden**.

Beim Beenden von ViPNet SafeDisk trennt das Programm alle eingebundenen Container. Wenn aus irgendwelchen Gründen einige Container nicht getrennt werden können (zum Beispiel, weil die im Container enthaltenen Dateien von anderen Anwendungen benutzt werden), wird vom Programm eine entsprechende Warnung ausgegeben.

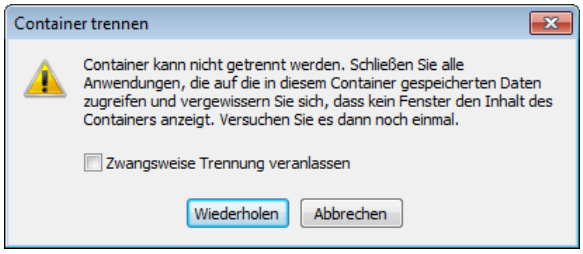
Container trennen
Container kann nicht getrennt werden. Schließen Sie alle Anwendungen, die auf die in diesem Container gespeicherten Daten zugreifen und vergewissern Sie sich, dass kein Fenster den Inhalt des Containers anzeigt. Versuchen Sie es dann noch einmal.
Zwangsweise Trennung veranlassen
Wiederholen
Abbrechen

Abbildung 10: Meldung über das Auftreten eines Fehlers beim Trennen eines Containers

Beim Einblenden einer solchen Meldung:

1 Stellen Sie sicher, dass die im Container enthaltenen Dateien nicht von anderen Programmen verwendet werden, und klicken Sie auf **Wiederholen**.

2 Um die Container zwangsweise zu trennen, aktivieren Sie im Meldungsfenster das Kontrollkästchen **Zwangsweise Trennung veranlassen** und klicken Sie auf **Wiederholen**. Das Programm blendet eine Warnung über möglichen Datenverlust ein.

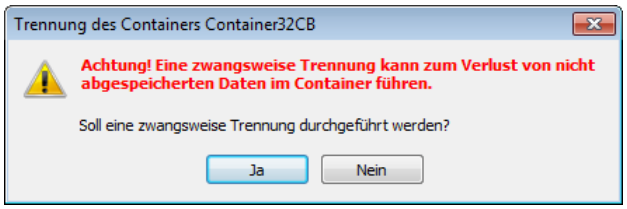
Trennung des Containers Container32CB
Achtung! Eine zwangsweise Trennung kann zum Verlust von nicht abgespeicherten Daten im Container führen.
Soll eine zwangsweise Trennung durchgeführt werden?
Ja
Nein

Abbildung 11: Warnung über möglichen Datenverlust

3 Stellen Sie sicher, dass alle im Container enthaltenen Daten abgespeichert sind, und klicken Sie im Meldungsfenster auf **Ja**.

Hinweis. Wenn die im Container enthaltenen Daten nicht abgespeichert werden, kann dies bei einer zwangsweisen Trennung des Containers zum Datenverlust führen.

Deinstallation von ViPNet SafeDisk

Bevor Sie ViPNet SafeDisk deinstallieren:

1. Erstellen Sie eine Sicherungskopie Ihrer vertraulichen Daten. Führen Sie dazu einen der folgenden Schritte aus:
   - Kopieren Sie die Container-Dateien und die Sicherungskopien der Containerschlüssel an einen sicheren Ort.
   - Erstellen Sie Export-Dateien für alle Ihre Container und kopieren Sie diese an einen sicheren Ort.
2. Wenn Sie nicht wollen, dass auf dem Computer Spuren sensibler Daten übrigbleiben:
   - Verwenden Sie die Bereinigungsfunktion von ViPNet SafeDisk (s. Spurenbeseitigung bei der Arbeit mit privaten Daten auf Seite 143).
   - Aktivieren Sie den „Extreme Gefahr“ Modus (s. Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus auf Seite 139) und löschen Sie alle Ihre Container und Containerschlüssel.

Zum Deinstallieren von ViPNet SafeDisk:

1. Melden Sie sich im Programm ab (s. ViPNet SafeDisk beenden auf Seite 30).
2. Öffnen Sie über das Menü **Start** die **Systemsteuerung**. Klicken Sie dort auf **Programme und Funktionen** (in Windows XP auf **Software**).
3. Wählen Sie in der Liste der installierten Programme den Eintrag **ViPNet SafeDisk** und klicken Sie auf **Ändern/Entfernen**. Es wird der Assistent **Hinzufügen/Entfernen** gestartet.
4. Aktivieren Sie das Optionsfeld **Alle Komponenten entfernen** und klicken auf **Weiter**.
5. Auf der Seite **Vorbereitung abgeschlossen** klicken Sie auf **Fertig**. Es wird eine Meldung über verbliebene Dateien und Ordner des Benutzers eingeblendet.

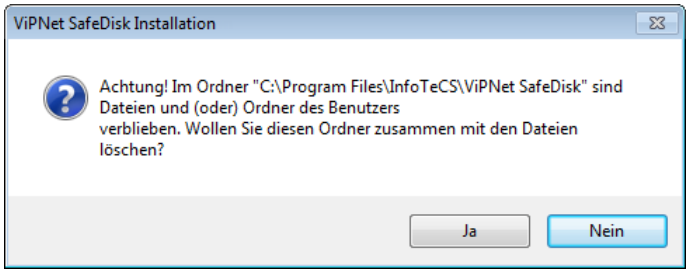
ViPNet SafeDisk Installation
Achtung! Im Ordner "C:\Program Files\InfoTeCS\ViPNet SafeDisk" sind Dateien und (oder) Ordner des Benutzers verblieben. Wollen Sie diesen Ordner zusammen mit den Dateien löschen?
Ja
Nein

Abbildung 12: Meldung über übriggebliebene Dateien und Ordner des Benutzers

6 Wenn Sie vorhaben, in Zukunft wieder mit den Containern zu arbeiten, klicken Sie auf **Nein**. Wenn Sie auf **Ja** klicken, werden die Daten vollständig gelöscht.

7 Damit der Vorgang der Deinstallation von ViPNet SafeDisk abgeschlossen werden kann, muss der Computer neu gestartet werden. Klicken Sie im Fenster mit der Meldung über einen möglichen Neustart des Computers auf die Schaltfläche **Jetzt neu starten**, um den Rechner sofort nach Abschluss der Deinstallation neu zu starten.

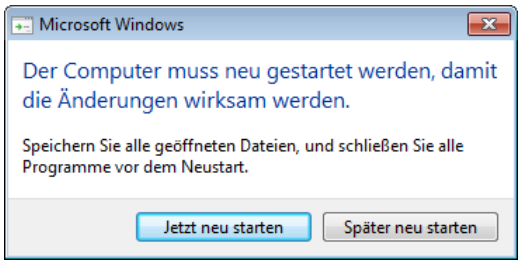
Microsoft Windows
Der Computer muss neu gestartet werden, damit die Änderungen wirksam werden.
Speichern Sie alle geöffneten Dateien, und schließen Sie alle Programme vor dem Neustart.
Jetzt neu starten
Später neu starten

Abbildung 13: Benachrichtigung über den Neustart

Wenn Sie den Computer zu einem späteren Zeitpunkt neu starten wollen, klicken Sie auf **Später neu starten**.

3

Arbeit mit ViPNet SafeDisk beginnen

ViPNet SafeDisk zum ersten Mal starten	36
Benutzerpasswort definieren	37
Benutzerpasswort ändern	40

ViPNet SafeDisk zum ersten Mal starten

Nach der Installation von ViPNet SafeDisk können Sie Ihre sensiblen Daten schützen. Um mit dem Schutz der Daten zu beginnen:

- Starten Sie ViPNet SafeDisk (ViPNet SafeDisk zum ersten Mal starten);
- Definieren Sie das Benutzerpasswort.

Um die Arbeit mit ViPNet SafeDisk zu beginnen:

1. Starten Sie das Programm (s. ViPNet SafeDisk starten auf Seite 29). Das Fenster **Benutzerpasswort SafeDisk** öffnet sich.

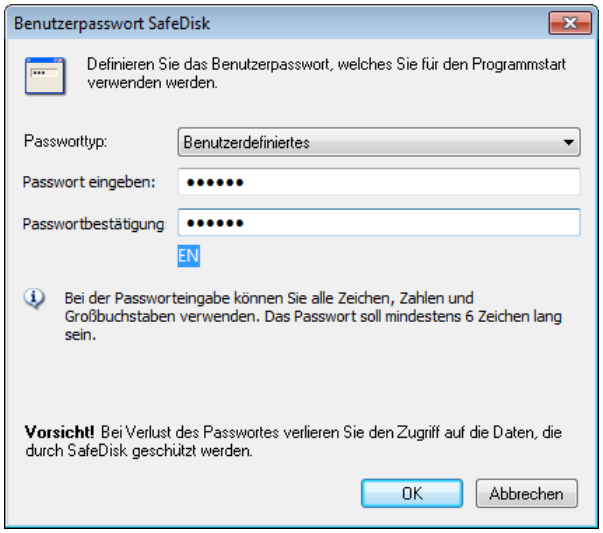
Benutzerpasswort SafeDisk
Definieren Sie das Benutzerpasswort, welches Sie für den Programmstart verwenden werden.
Passworttyp:
Benutzerdefiniertes
Passwort eingeben:
Passwortbestätigung
EN
Bei der Passworteingabe können Sie alle Zeichen, Zahlen und Großbuchstaben verwenden. Das Passwort soll mindestens 6 Zeichen lang sein.
Vorsicht! Bei Verlust des Passwortes verlieren Sie den Zugriff auf die Daten, die durch SafeDisk geschützt werden.
OK
Abbrechen

Abbildung 14: Fenster Benutzerpasswort SafeDisk

2. Definieren Sie Ihr Passwort, wie in den Abschnitten Eigenes Passwort definieren (auf Seite 37) und Zufälliges Passwort generieren (auf Seite 38).
3. Klicken Sie auf **OK**. Das Hauptfenster von ViPNet SafeDisk öffnet sich.
4. Setzen Sie Ihre Arbeit fort, wie im Abschnitt Datenschutz mit Hilfe von ViPNet SafeDisk (auf Seite 58) beschrieben ist.

Benutzerpasswort definieren

Das von Ihnen festgelegte Passwort wird für die Anmeldung im Programm ViPNet SafeDisk verwendet, deswegen empfehlen wir, ein sicheres und gut bedachtes Passwort auszusuchen.

Dazu können Sie die Funktion zur Erzeugung zufälliger Passwörter verwenden (s. Zufälliges Passwort generieren auf Seite 38) oder ein eigenes Passwort definieren (s. Eigenes Passwort definieren auf Seite 37).

Achtung! Beim Verlust des Passworts besteht keine Möglichkeit, auf die geschützten Daten in ViPNet SafeDisk zuzugreifen.

Eigenes Passwort definieren

1 Im Fenster **Benutzerpasswort SafeDisk** unter **Passworttyp** wählen Sie **Benutzerdefiniert**.

2 Geben Sie das Passwort ein und bestätigen dieses in entsprechenden Feldern. Beim Erstellen des Passworts können Sie beliebige Groß- und Kleinbuchstaben, Ziffern und andere Symbole verwenden.

Achtung! Es darf kein Passwort mit einer Länge von 32 Symbolen erstellt werden. Passwörter dieser Länge können in den laufenden Versionen der ViPNet Anwendungen nicht verwendet werden. Diese Einschränkung ist bedingt durch den bestehenden Algorithmus zur Weiterleitung des Passworts an den Cryptoprovider. In Übereinstimmung mit diesem Algorithmus darf die Länge des Passworts nicht mehr als 31 Zeichen betragen.

3 Klicken Sie auf **OK**.

Tipp. Wird raten ausdrücklich davon ab, persönliche Daten (Name, Familienname, Geburtsdatum, Telefonnummer) oder verbreitete Kennwörter (zum Beispiel password, qwerty, asdfgh und so weiter) beim Anlegen des Passworts zu verwenden.

Zufälliges Passwort generieren

1 Im Fenster **Benutzerpasswort SafeDisk** unter Passworttyp wählen Sie **Zufälliges**.

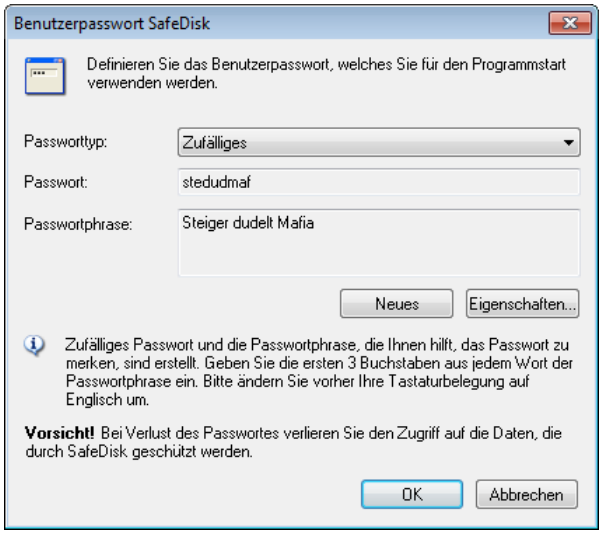
Benutzerpasswort SafeDisk
Definieren Sie das Benutzerpasswort, welches Sie für den Programmstart verwenden werden.
Passworttyp:
Zufälliges
Passwort:
stedudmaf
Passwortphrase:
Steiger dudelt Mafia
Neues
Eigenschaften...
Zufälliges Passwort und die Passwortphrase, die Ihnen hilft, das Passwort zu merken, sind erstellt. Geben Sie die ersten 3 Buchstaben aus jedem Wort der Passwortphrase ein. Bitte ändern Sie vorher Ihre Tastaturbelegung auf Englisch um.
Vorsicht! Bei Verlust des Passwortes verlieren Sie den Zugriff auf die Daten, die durch SafeDisk geschützt werden.
OK
Abbrechen

Abbildung 15: Zufälliges Passwort

2 Es wird das digitale Roulette (auf Seite 179) – ein Zufallszahlengenerator – gestartet. Zufallszahlen werden dazu verwendet, ein zufälliges Passwort zu erstellen. Das digitale Roulette wird in ViPNet SafeDisk nur dann gestartet, wenn zum ersten Mal zufällige Zahlen benötigt werden.

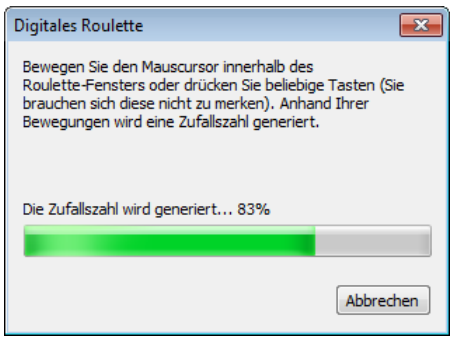
Digitales Roulette
Bewegen Sie den Mauscursor innerhalb des Roulette-Fensters oder drücken Sie beliebige Tasten (Sie brauchen sich diese nicht zu merken). Anhand Ihrer Bewegungen wird eine Zufallszahl generiert.
Die Zufallszahl wird generiert... 83%
Abbrechen

Abbildung 16: Digitales Roulette

3 Folgen Sie den Anweisungen im Fenster **Digitales Roulette**. Das zufällige Passwort wird generiert.

Wenn Sie ein anderes Zufallspasswort bevorzugen, klicken Sie auf **Anderes**.

Tipp. Die Passwortphrase ist eine Eselsbrücke und hilft Ihnen, dass Passwort zu merken. Für das Passwort werden die ersten Buchstaben aus jedem Wort im Satz genommen. Zum Beispiel, dem Satz „Steiger dudelt Mafia“ entspricht das Passwort

stedudmaf.

Eigenschaften des zufälligen Passwortes ändern

Wenn Sie die Eigenschaften des zufälligen Passwortes ändern wollen:

1. Im Fenster **Benutzerpasswort SafeDisk** klicken Sie auf **Eigenschaften** (als Passworttyp muss dafür **Zufälliges** gewählt sein). Das Fenster Eigenschaften des zufälligen Passwortes öffnet sich.

Abbildung 17: Eigenschaften zufälliger Passwörter

   - Aus der Dropdown-Liste **Sprache** wählen Sie die Sprache: **Russisch**, **Deutsch**, **Französisch** oder **English**.
   - Wählen Sie die gewünschte **Anzahl der Wörter in der Passwortphrase** und **Anzahl der Buchstaben** aus jedem Wort.

2. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Benutzerpasswort ändern

Es wird empfohlen, das Passwort regelmäßig zu ändern, um die Sicherheit zu erhöhen.

Achtung! Wenn Sie vor dem Passwortwechsel eine Sicherungskopie der Konfiguration erstellen (s. Sicherungskopie der Konfiguration erstellen auf Seite 112) und diese später nutzen wollen, merken Sie sich das alte Passwort.

Um das Benutzerpasswort zu ändern:

1. Im Menüpunkt **Sicherheit** wählen Sie **Passwort ändern**.
2. Wenn die Container eingebunden sind erscheint eine Meldung, dass sie getrennt werden sollen, um fortzufahren. Klicken Sie auf **Ja**.
3. Das Fenster Benutzerpasswort SafeDisk öffnet sich.
4. Geben Sie das neue Passwort ein (s. Benutzerpasswort definieren auf Seite 37).

4

Registrierung von ViPNet SafeDisk

Vor der Registrierung von ViPNet SafeDisk	42
Seriennummer anfordern	44
Registrierungscode anfordern	45
ViPNet SafeDisk registrieren	54
Vorgehensweise bei der Registrierung per Registrierungsdatei	57

Vor der Registrierung von ViPNet SafeDisk

Warum ViPNet SafeDisk registriert werden sollte

Nach der Installation von ViPNet SafeDisk arbeitet das Programm zunächst als Free Edition (s. Einschränkungen der kostenlosen Version auf Seite 16). ViPNet SafeDisk kann jederzeit registriert werden. Danach steht der volle Funktionsumfang des Programms ohne zeitliche Einschränkungen zur Verfügung.

Folgende Vorgangsweise wird empfohlen:

- installieren Sie ViPNet SafeDisk und nutzen Sie die nicht registrierte Version des Programms, um die Möglichkeiten und Vorteile des Produkts kennenzulernen;
- registrieren Sie Ihre Kopie von ViPNet SafeDisk.

Registrierung starten

Sie können ViPNet SafeDisk selbst registrieren (individuelle Registrierung). Führen Sie dafür die nachfolgenden Anweisungen aus.

Wenn Sie als Systemadministrator mehrere Kopien des Programms registrieren wollen, nutzen Sie die Gruppenregistrierung. Dabei werden die Registrierungsanfragen aller Benutzer gesammelt und als eine E-Mail gesendet. Im nächsten Schritt erhalten Sie alle Registrierungscodes auf einmal. Mehr über die Gruppenregistrierung lesen Sie im Abschnitt Vorgehensweise bei der Registrierung per Registrierungsdatei (auf Seite 57).

Hinweis. Wenn ViPNet SafeDisk erneut auf einem Rechner installiert wurde, auf dem es bereits registriert war, können Sie die in der Datei *.brg gespeicherten Registrierungsdaten benutzen (s. Registrierungsdaten speichern auf Seite 55).

Wenn Sie Änderungen an der Konfiguration des Rechners vorgenommen haben, auf dem ViPNet SafeDisk, im Einsatz ist, lesen Sie bitte den Abschnitt Wenn sich die Konfiguration Ihres Rechners geändert hat (auf Seite 56).

Führen Sie folgende Schritte aus, um ViPNet SafeDisk zu registrieren:

1 Klicken Sie im Hauptfenster von ViPNet SafeDisk im Menü **Hilfe** auf den Eintrag **Registrierung**. Es wird der Assistent **ViPNet SafeDisk Registrierung** gestartet.

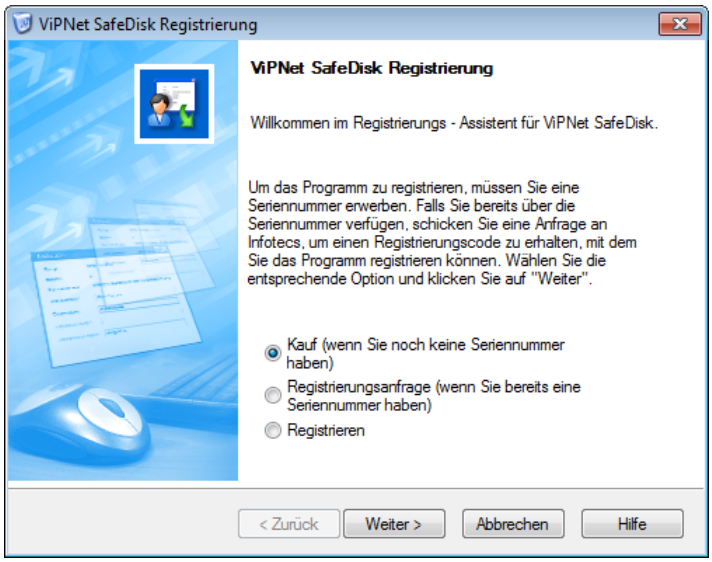
ViPNet SafeDisk Registrierung
ViPNet SafeDisk Registrierung
Willkommen im Registrierungs - Assistent für ViPNet SafeDisk.
Um das Programm zu registrieren, müssen Sie eine Seriennummer erwerben. Falls Sie bereits über die Seriennummer verfügen, schicken Sie eine Anfrage an Infotecs, um einen Registrierungscode zu erhalten, mit dem Sie das Programm registrieren können. Wählen Sie die entsprechende Option und klicken Sie auf "Weiter".
Kauf (wenn Sie noch keine Seriennummer haben)
Registrierungsanfrage (wenn Sie bereits eine Seriennummer haben)
Registrieren
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 18: ViPNet SafeDisk Registrierung

2 Wenn Sie zu diesem Zeitpunkt:

- ViPNet SafeDisk noch nicht gekauft haben, wählen Sie die Option **Kauf (wenn Sie noch keine Seriennummer haben)** (s. Seriennummer anfordern auf Seite 44).

Hinweis. Wenn Sie ViPNet SafeDisk auf einer CD erworben haben, dann verfügen Sie bereits über eine Seriennummer (diese ist gemeinsam mit der CD im Paket enthalten), und können unmittelbar zur Anfrage des Registrierungscodes übergehen (siehe unten).

- ViPNet SafeDisk bereits gekauft haben und über eine Seriennummer verfügen, wählen Sie **Registrierungsanfrage (wenn Sie bereits eine Seriennummer haben)** (s. Registrierungscode anfordern auf Seite 45).

Hinweis. Wenn Sie eine Registrierungsanfrage über das Internet gesendet haben, erfolgt die Registrierung von ViPNet SafeDisk automatisch ohne weitere Mitwirkung Ihrerseits.

- ViPNet SafeDisk bereits gekauft und einen Registrierungscode erhalten haben, wählen Sie **Registrieren** (s. ViPNet SafeDisk registrieren auf Seite 54).

Seriennummer anfordern

Zum Anfordern einer Seriennummer:

1. Wählen Sie im Assistentenfenster **ViPNet SafeDisk Registrierung** die Option **Kauf (wenn Sie noch keine Seriennummer haben)** und klicken auf **Weiter**.

   In Ihrem Browser wird die Website für die Bestellung von ViPNet-Produkten von Infotecs geöffnet. Erwerben Sie ViPNet SafeDisk über die Website. Sie erhalten die Seriennummer per E-Mail.

2. Kehren Sie nach Erhalt der Seriennummer zum Assistenten **ViPNet SafeDisk Registrierung** zurück und führen Sie die Anfrage des Registrierungscodes durch (s. Registrierungscode anfordern auf Seite 45).

Registrierungscode anfordern

Zum Anfordern eines Registrierungscodes für ViPNet SafeDisk:

1. Wählen Sie im Assistentenfenster **ViPNet SafeDisk Registrierung** die Option **Registrierungsanfrage (wenn Sie bereits eine Seriennummer haben)** und klicken auf **Weiter**.
2. Wählen Sie im Fenster **Möglichkeiten der Registrierungsanfrage** die für Sie passende Option aus. Aktivieren Sie dazu eines der folgenden Optionsfelder:
   - **Über das Internet (online)** (s. Registrierungsanfrage über das Internet auf Seite 45).
   - **Via E-Mail** (s. Registrierungsanfrage via E-Mail auf Seite 48).
   - **Per Telefon** (s. Registrierungsanfrage per Telefon auf Seite 50).
   - **Per Registrierungsdatei** (s. Registrierungsanfrage per Registrierungsdatei auf Seite 51).

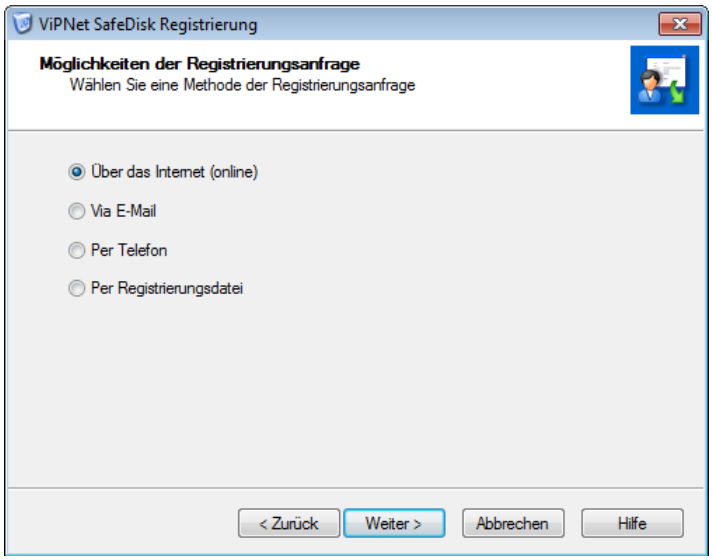

Abbildung 19: Möglichkeiten der Registrierungsanforderung

3. Klicken Sie auf **Weiter**.

Registrierungsanfrage über das Internet

Achtung! Für diese Registrierungsmöglichkeit ist ein Internet-Zugang erforderlich.

Wenn Sie die Registrierungsoption **Über das Internet (online)** gewählt haben, wird das Fenster **Registrierungsdaten** eingeblendet.

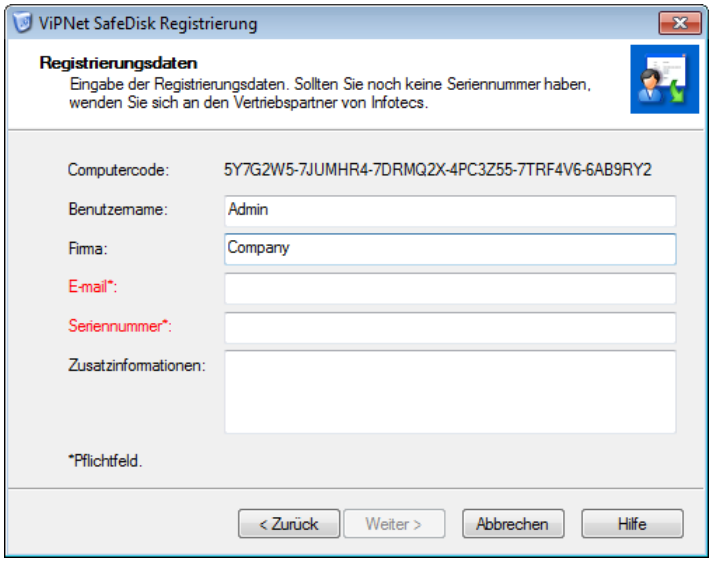

Abbildung 20: Registrierungsdaten eingeben

Führen Sie im Fenster **Registrierungsdaten** folgende Schritte aus:

1 Geben Sie im Feld **Seriennummer** die Seriennummer ein.

Hinweis. Wenn Sie über keine Seriennummer verfügen, fordern Sie diese zunächst an (s. Seriennummer anfordern auf Seite 44).

Wenn Sie die Seriennummer zu einem früheren Zeitpunkt bereits eingegeben haben, so erscheint diese hier automatisch.

2 Geben Sie im Feld **Benutzername** Ihren Namen ein. Dieser wird für die Herausgabe der Lizenz und für die Ansprache verwendet. Dieses Feld muss nicht ausgefüllt werden. Standardmäßig wird im Feld **Benutzername** der Name eingeblendet, den Sie während der Installation von ViPNet SafeDisk angegeben haben.

3 Geben Sie im Feld **Firma** den Namen Ihrer Firma ein. Dieses Feld muss nicht ausgefüllt werden. Standardmäßig wird im Feld **Firma** der Firmenname eingeblendet, den Sie während der Installation von ViPNet SafeDisk angegeben haben.

4 Geben Sie im Feld **E-Mail** ihre E-Mail-Adresse ein. Diese wird in besonderen Fällen für eine Kontaktaufnahme genutzt.

Achtung! Ihre E-Mail-Adresse wird von uns weder verkauft noch weiterverbreitet. Die Firma „INFOTECS nimmt den Schutz Ihrer persönlichen Daten sehr ernst und trifft alle Maßnahmen zur Verhinderung von unberechtigtem Zugriff auf Daten und unerlaubter Weiterleitung von Informationen.

5 Im Feld **Zusatzinformationen** können Sie beliebige zusätzliche Anmerkungen angeben, zum Beispiel Ihre Kontaktdaten, Meldungen über mögliche Probleme oder Anregungen, die sich auf ViPNet Software beziehen.

Im Feld **Computercode** wird ein Code eingeblendet, der Ihren Rechner eindeutig identifiziert. Der Wert in diesem Feld kann nicht geändert werden.

6 Klicken Sie auf die Schaltfläche **Weiter**. Es wird ein Fenster geöffnet, das den Status der Registrierungsanfrage anzeigt. Hier wird die Zeit seit dem Beginn des laufenden Versuchs einer Registrierungsanfrage hochgezählt. Beachten Sie, dass für den Aufbau einer Verbindung nicht mehr als 3 Minuten veranschlagt sind.

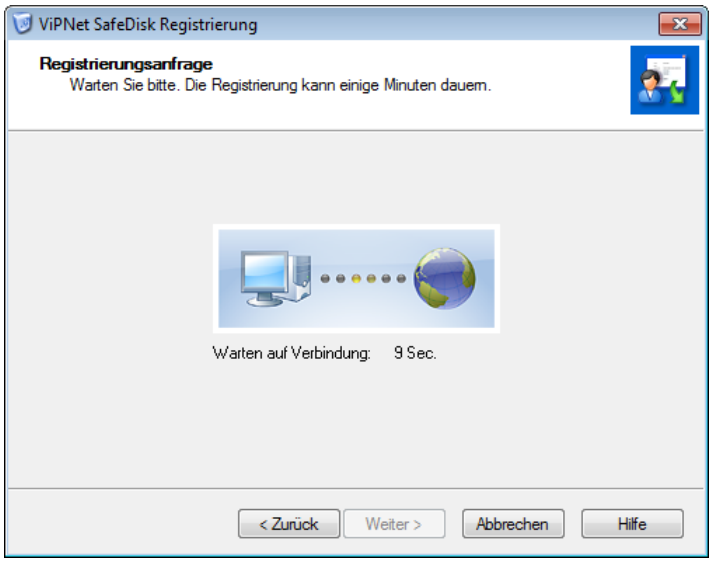

Abbildung 21: Verlauf der Registrierungsanfrage

Wenn innerhalb von 3 Minuten kein Verbindungsaufbau zum Server des Registrierungssystems von „INFOTECS“ erfolgt, wird eine entsprechende Meldung eingeblendet.

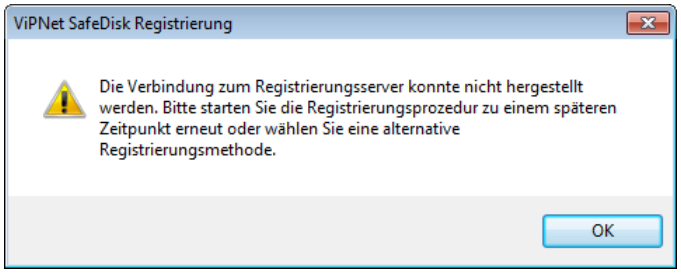
ViPNet SafeDisk Registrierung
Die Verbindung zum Registrierungsserver konnte nicht hergestellt werden. Bitte starten Sie die Registrierungsprozedur zu einem späteren Zeitpunkt erneut oder wählen Sie eine alternative Registrierungsmethode.
OK

Abbildung 22: Fehlermeldung bei fehlender Verbindung zum Server

Wenn die Verbindung zum Server des Registrierungssystems erfolgreich hergestellt wurde, aber die von Ihnen angegebenen Daten nicht korrekt sind, gibt das Programm eine diesbezügliche Meldung aus.

Klicken Sie im Meldungsfenster auf **OK**. Sie kehren zum Assistentenfenster **Registrierungsdaten** zurück.

Wenn die Registrierung verweigert wurde, wird wieder das Fenster **Registrierungsdaten** geöffnet. Überprüfen Sie die Richtigkeit der eingegebenen Seriennummer und versuchen Sie es erneut.

Wenn die Registrierung erfolgreich durchgeführt wurde, wird das Fenster **Die Registrierung von ViPNet SafeDisk wurde erfolgreich abgeschlossen** eingeblendet. In diesem Fenster sind Empfehlungen für eine sichere Speicherung Ihrer Registrierungsdaten angegeben (s. Registrierungsdaten speichern auf Seite 55).

7 Klicken Sie auf **Fertig**.

Registrierungsanfrage via E-Mail

Achtung! Für diese Registrierungsmöglichkeit ist ein Internet-Zugang und ein E-Mail Client erforderlich.

Wenn Sie die Registrierungsoption **Via E-Mail** gewählt haben, wird das Fenster **Registrierungsdaten** geöffnet. Im Fenster **Registrierungsdaten**:

1 Geben Sie alle Daten ein, wie im Abschnitt Registrierungsanfrage über das Internet (auf Seite 45) beschrieben.

2 Klicken Sie auf **Weiter**. In Ihrem E-Mail-Programm wird eine neue Nachricht erstellt, die die von Ihnen angegebenen Registrierungsdaten enthält. Die E-Mail wird an den Empfänger reg@infotecs.biz adressiert.

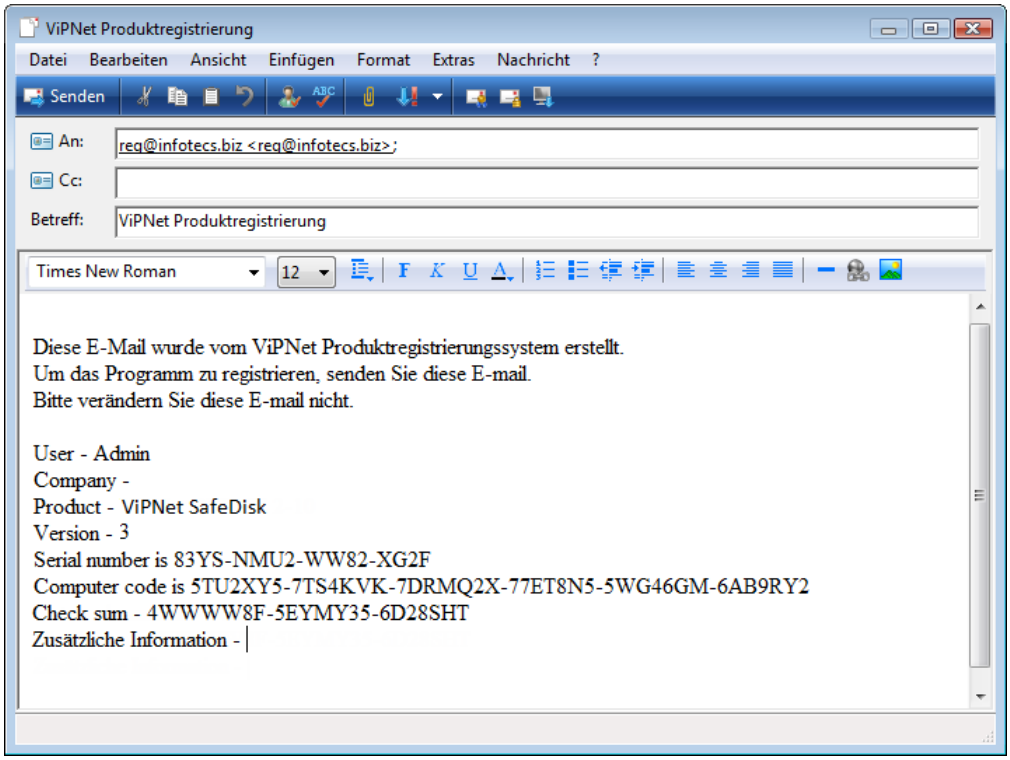

Abbildung 23: Registrierungscode via E-Mail anfordern

Achtung! Es wird empfohlen, die Nachricht mit den Registrierungsdaten nicht zu editieren.

3 Zum Abschließen der Registrierung senden Sie die E-Mail ab. Nach Überprüfung Ihrer Registrierungsdaten erhalten Sie den Registrierungscode via E-Mail.

Achtung! Wenn Sie innerhalb weniger Tage keine Rückmeldung von „INFOTECS erhalten, versuchen Sie erneut, die Nachricht zu versenden. Dazu wiederholen Sie alle Schritte, die in diesem Abschnitt beschrieben sind. Wenn auch das nicht zu einer Registrierung von ViPNet SafeDisk geführt hat, setzen Sie sich mit dem Kundendienst von „INFOTECS in Verbindung.

4 Nach Erhalt der E-Mail mit dem Registrierungscode registrieren Sie Ihre Kopie von ViPNet SafeDisk (s. ViPNet SafeDisk registrieren auf Seite 54).

Registrierungsanfrage per Telefon

Wenn Sie die Registrierungsoption **Per Telefon** gewählt haben, wird das Fenster **Registrierungsanforderung per Telefon** geöffnet.

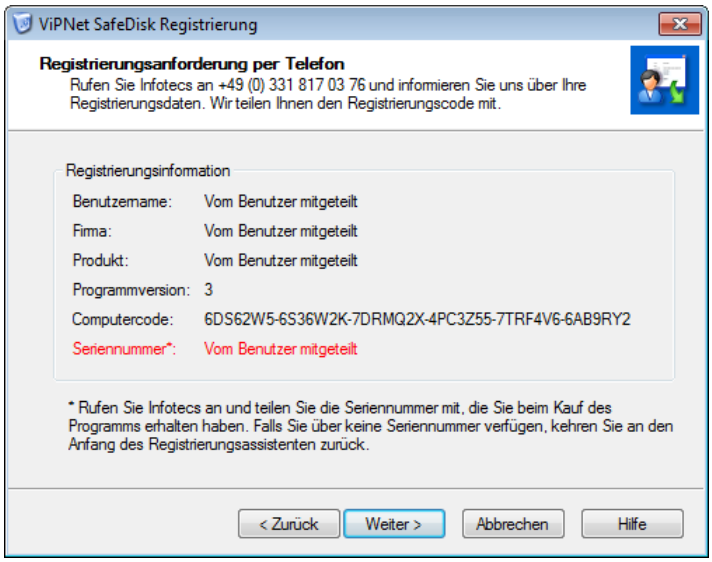
ViPNet SafeDisk Registrierung
Registrierungsanforderung per Telefon
Rufen Sie Infotecs an +49 (0) 331 817 03 76 und informieren Sie uns über Ihre Registrierungsdaten. Wir teilen Ihnen den Registrierungscode mit.
Registrierungsinformation
Benutzername: Vom Benutzer mitgeteilt
Firma: Vom Benutzer mitgeteilt
Produkt: Vom Benutzer mitgeteilt
Programmversion: 3
Computercode: 6DS62W5-6S36W2K-7DRMQ2X-4PC3Z55-7TRF4V6-6AB9RY2
Seriennummer*: Vom Benutzer mitgeteilt
* Rufen Sie Infotecs an und teilen Sie die Seriennummer mit, die Sie beim Kauf des Programms erhalten haben. Falls Sie über keine Seriennummer verfügen, kehren Sie an den Anfang des Registrierungsassistenten zurück.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 24: Registrierungsanforderung per Telefon

In diesem Fenster sind alle Daten angegeben, die Sie einem Mitarbeiter von Infotecs bei der Registrierung mitteilen müssen.

1. Rufen Sie Infotecs GmbH unter der im oberen Fensterbereich angegebenen Nummer an und teilen Sie Infotecs GmbH Ihre Registrierungsdaten mit. Als Antwort wird Ihnen der Registrierungscode mitgeteilt.
2. Nach Erhalt des Registrierungscodes klicken Sie auf **Weiter**. Es wird das Fenster **Registrieren** geöffnet.

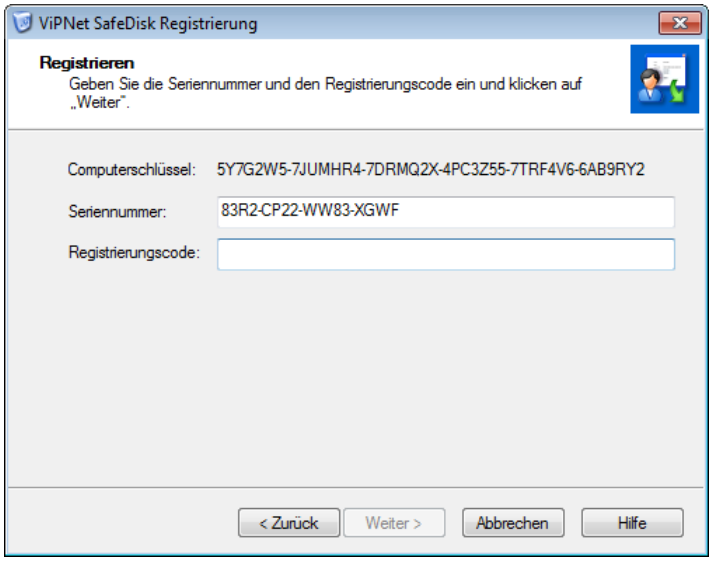

Abbildung 25: Fenster Registrieren

3 Geben Sie im Fenster **Registrieren** die Seriennummer und den Registrierungscode ein und klicken Sie auf **Weiter**.

Hinweis. Wenn Sie die Seriennummer zu einem früheren Zeitpunkt bereits eingegeben haben, wird das Feld **Seriennummer** automatisch ausgefüllt.

Wenn die eingegebenen Daten korrekt sind, wird das Fenster **Die Registrierung von ViPNet SafeDiskwurde erfolgreich abgeschlossen** eingeblendet. In diesem Fenster sind Empfehlungen für eine sichere Speicherung Ihrer Registrierungsdaten angegeben (s. Registrierungsdaten speichern auf Seite 55).

4 Klicken Sie auf **Fertig**.

Registrierungsanfrage per Registrierungsdatei

Die Registrierung über Textdatei wird für mehrere Benutzer durchgeführt. Dabei teilt jeder Benutzer dem Systemadministrator die Registrierungsdaten mit. Sie müssen den Registrierungscode nicht persönlich bei Infotecs anfordern.Verwenden Sie den Assistent **ViPNet SafeDisk Registrierung** um eine Registrierungsdatei für den Systemadministrator zu erstellen.

Hinweis. Wenn nur eine Kopie des Programms ViPNet SafeDisk über die Textdatei registriert werden soll, führen Sie zunächst die in diesem Abschnitt beschriebenen Schritte 1-6 durch. Weiters führen Sie die Aktionen des Systemadministrators aus dem Abschnitt Vorgehensweise bei der Registrierung über Textdatei (s. Vorgehensweise bei der Registrierung per Registrierungsdatei auf Seite 57) durch. Anschließend führen Sie den Schritt 7 durch, indem Sie Ihre Kopie von ViPNet SafeDisk registrieren (s. ViPNet SafeDisk registrieren auf Seite 54).

Nachdem die Registrierungsdaten aller Benutzer beim Systemadministrator eingegangen sind sendet er diese an Infotecs GmbH. Nach dem Erhalt der Registrierungscodes kann der Registrierungsvorgang an jedem Rechner einzeln abgeschlossen werden.

Um die Registrierung per Registrierungsdatei durchzuführen:

1. Im Fenster **Möglichkeiten der Registrierungsanfrage** wählen Sie **Per Registrierungsdatei**.

2. Auf der Seite **Registrierungsdaten** geben Sie alle notwendigen Informationen ein. Klicken Sie auf **Weiter**.

3. Im Fenster **Speicherung der Registrierungsdaten** klicken Sie auf **Durchsuchen** und definieren Sie einen Ordner in dem die Datei mit Registrierungsdaten gespeichert wird.

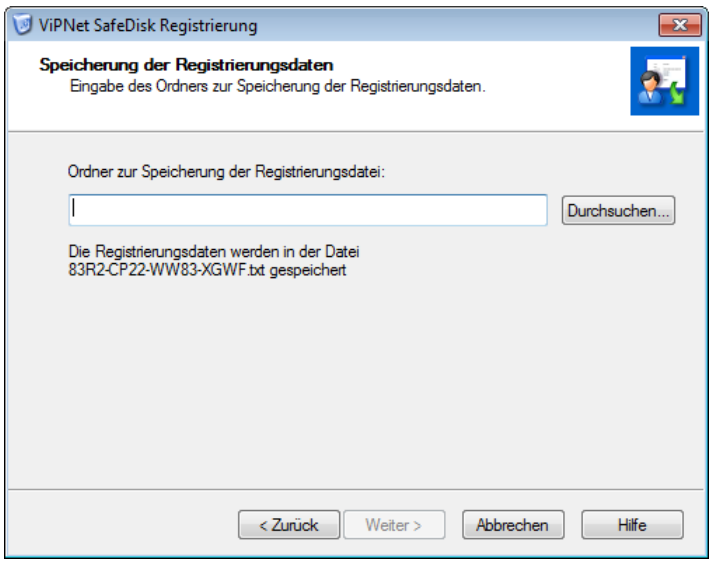

Abbildung 26: Speicherung der Registrierungsdaten

4. Nachdem Sie einen Ordner definiert haben, klicken Sie auf **Weiter**. Die Registrierungsdaten werden gespeichert, der Dateiname entspricht Ihrer Seriennummer: `<Seriennummer>.txt`.

Im nächsten Fenster klicken Sie auf **Fertig**.

5 Senden Sie die Datei mit den Registrierungsdaten Ihrem Systemadministrator.

6 Nachdem Sie den Registrierungscode vom Systemadministrator erhalten haben, schließen Sie den Registrierungsvorgang von ViPNet SafeDisk ab (s. ViPNet SafeDisk registrieren auf Seite 54).

ViPNet SafeDisk registrieren

Nachdem Sie von Infotecs GmbH den Registrierungscode erhalten haben, können Sie Ihre Kopie von ViPNet SafeDisk registrieren. Dazu:

1. Starten Sie den Assistenten **ViPNet SafeDisk Registrierung** (s. Registrierung starten auf Seite 42).
2. Wählen Sie im ersten Fenster die Option **Registrieren** und klicken Sie auf **Weiter**.
3. Geben Sie im Fenster **Seriennummer** die Seriennummer ein und klicken Sie auf **Weiter**.

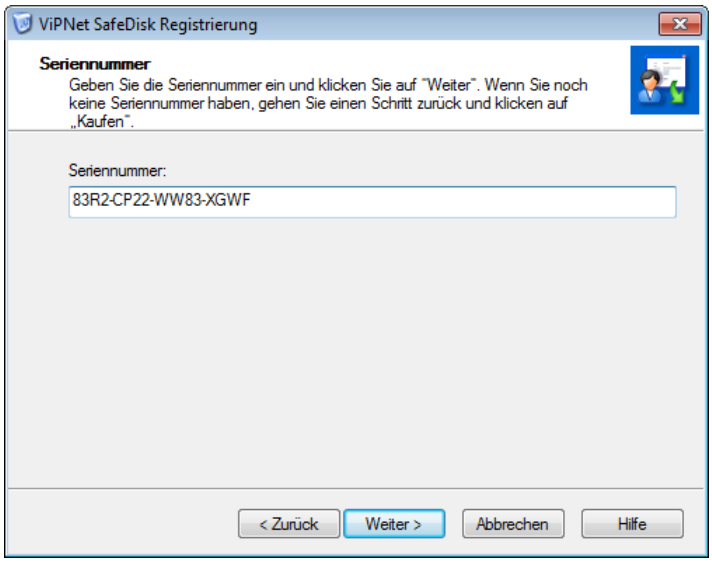
ViPNet SafeDisk Registrierung
Seriennummer
Geben Sie die Seriennummer ein und klicken Sie auf "Weiter". Wenn Sie noch keine Seriennummer haben, gehen Sie einen Schritt zurück und klicken auf „Kaufen".
Seriennummer:
83R2-CP22-WW83-XGWF
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 27: Fenster Seriennummer

Hinweis. Wenn Sie die Seriennummer zu einem früheren Zeitpunkt eingegeben haben, wird das Feld **Seriennummer** automatisch befüllt.

1. Im Fenster **Registrierungscode**:
   - Wenn Sie die Registrierung für einen Rechner durchführen, wählen Sie die Option **Einfache Registrierung** und geben Sie den Registrierungscode ein;
   - Wenn eine Gruppenregistrierung stattfand, wählen Sie die Option **Registrierung über Textdatei**, klicken Sie auf **Durchsuchen** und definieren die den Pfad zur Datei mit dem Registrierungscode.

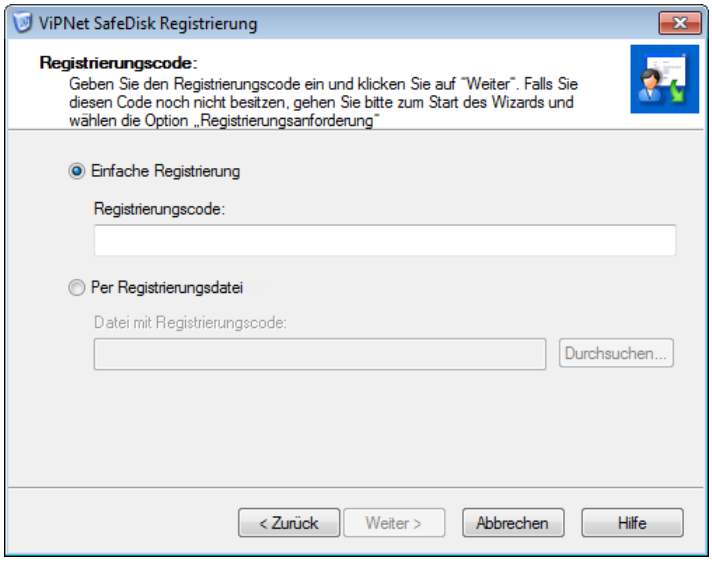
ViPNet SafeDisk Registrierung
Registrierungscode:
Geben Sie den Registrierungscode ein und klicken Sie auf "Weiter". Falls Sie diesen Code noch nicht besitzen, gehen Sie bitte zum Start des Wizards und wählen die Option „Registrierungsanforderung"
Einfache Registrierung
Registrierungscode:
Per Registrierungsdatei
Datei mit Registrierungscode:
Durchsuchen...
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 28: Eingabe des Registrierungscodes

2 Klicken Sie auf **Weiter**. Wenn die von Ihnen eingegebenen Daten korrekt sind, wird das Fenster **Die Registrierung von ViPNet SafeDisk wurde erfolgreich abgeschlossen** geöffnet.

3 Klicken Sie auf **Fertig**.

4 Speichern Sie die Registrierungsdaten (s. Registrierungsdaten speichern auf Seite 55), indem Sie die Datei *.brg, die sich im Installationsordner von ViPNet SafeDisk befindet, an einen sicheren Ort kopieren.

Registrierungsdaten speichern

Nach Abschluss der Registrierung speichert das Programm die Registrierungsdaten in der Datei `*.brg`, die im folgenden Ordner:

- `C:\ProgramData\InfoTeCS\ViPNet SafeDisk\`, für Betriebssysteme Windows Vista, Windows 7 oder Windows Server 2008;
- `C:\Documents and Settings\All Users\Application Data\InfoTeCS\ViPNet SafeDisk\`, für Betriebssysteme Windows XP oder Windows Server 2003.

Hinweis. Der Name der Datei `*.brg` hängt von der Version der ViPNet-Software ab.

Wir empfehlen, die Datei mit Registrierungsdaten an einen sicheren Ort zu kopieren, da diese Datei bei einer wiederholten Installation von ViPNet SafeDisk (wenn Sie zum Beispiel das Programm in einem anderen Ordner neu installieren möchten oder wenn das Programm nach einer Formatierung der Festplatte erneut installiert werden soll) von Nutzen sein kann. In diesem Fall beenden Sie das Programm, kopieren die gesicherte Datei `*.brg` in den oben beschriebenen Ordner und started das Programm erneut. Nach einem Start wird das Programm automatisch registriert (wenn die Registrierungsdaten korrekt sind, und sich die Konfiguration des Rechners nicht geändert hat).

Die Registrierungsdaten (Seriennummer, Computercode, u. s. w.) werden auch in der Logdatei der Registrierung `reginfo.txt` gespeichert, die im Installationsordner von ViPNet SafeDisk angelegt wird. Sie können die in dieser Datei enthaltenen Daten dazu verwenden, das Programm nach einer Neuinstallation manuell zu registrieren (wenn zum Beispiel die Datei `*.brg` verloren geht).

Wenn sich die Konfiguration Ihres Rechners geändert hat

Eine Erneuerung der Konfiguration des Computers, auf dem ViPNet SafeDisk installiert ist, kann Auswirkungen auf die Funktionsweise des Programms haben. Wenn die Änderungen signifikant sind (es wurde zum Beispiel ein Großteil der Komponenten ersetzt), muss Ihre Kopie von ViPNet SafeDisk neu registriert werden (s. Registrierungscode anfordern auf Seite 45). Wenn die Änderungen in der Konfiguration des Rechners unwesentlich sind, muss ViPNet SafeDisk nicht neu registriert werden.

Beim ersten Start von ViPNet SafeDisk nach einer unwesentlichen Änderung der Rechnerkonfiguration wird vom Programm die Meldung ausgegeben, dass aufgrund einer Änderung der Rechnerkonfiguration eine neue `*.brg` Datei erzeugt wurde. Das bedeutet, dass die ursprüngliche Registrierungsdatei veraltet ist, und Sie die Datei nicht mehr für eine erneute Registrierung des Programms nach einer Neuinstallation verwenden können.

Kopieren Sie die neue Datei `*.brg` an einen sicheren Ort. Wenn Sie ViPNet SafeDisk neu installieren, kopieren Sie diese Datei in den Installationsordner von ViPNet SafeDisk und das Programm wird automatisch registriert.

Vorgehensweise bei der Registrierung per Registrierungsdatei

Während der Registrierung per Registrierungsdatei werden die Registrierungscodes für mehrere PCs gleichzeitig im Regelfall vom Systemadministrator beantragt.

Vor dem Beginn der Registrierung per Registrierungsdatei muss für jeden PC mit installiertem ViPNet SafeDisk eine Seriennummer vorhanden sein. Wenn das nicht der Fall ist, können die Seriennummer mit Hilfe des Registrierungsassistenten ViPNet SafeDisk gekauft werden (s. Seriennummer anfordern auf Seite 44).

Auf jedem PC wird ein Antrag auf die Registrierung per Registrierungsdatei erstellt (s. Registrierungsanfrage per Registrierungsdatei auf Seite 51). Als Ergebnis wird eine Textdatei `*.txt` generiert, welche die Daten für die Registrierung per Registrierungsdatei beinhaltet.

Wenn Sie die Registrierung per Registrierungsdatei durchführen:

1. Speichern Sie alle Dateien mit Registrierungsdaten in einem Ordner.
2. Verbinden Sie alle Dateien in eine Datei mit dem Befehl: `copy *.txt registration.all`. Anstatt `registration.all` können Sie einen beliebigen Dateinamen verwenden.
3. Senden Sie die neu generierte Datei an die E-Mail adresse reg@infotecs.biz. Als Betreff geben Sie ViPNet Group Registration ein.
4. Nach der Bearbeitung Ihrer Anfrage bei Infotecs GmbH erhalten Sie eine E-Mail mit der angehängten Textdatei `*.txt`. Die Datei wird die Registrierungscodes für alle PC´s erhalten. Anschließend kann die Registrierung auf jedem PC einzeln abgeschlossen werden.

5

Datenschutz mit Hilfe von ViPNet SafeDisk

Vorgehensweise beim Datenschutz	60
Container erstellen	61
Sicherungskopie der Container-Schlüssel	69
Container einbinden	74
Container formatieren	79
Tägliche Arbeit mit den geschützten Daten	81
Container trennen	83
Containereigenschaften ansehen und ändern	85
Containerschlüssel aktualisieren	88
Container-Datei verschieben	90
Container löschen	91

Parameter von ViPNet SafeDisk einstellen 92

Vorgehensweise beim Datenschutz

Für den erfolgreichen Schutz von Daten und die Sicherstellung eines sicheren Zugangs zu Informationen müssen alle Schritte aus der nachfolgenden Liste durchgeführt werden.

Hinweis. Einige Punkte dieser Liste beziehen sich auf die Unterpunkte verschiedener Abschnitte. Nach der Durchführung der Unterpunkte wechseln Sie zum nächsten Schritt aus der Liste.

Wenn die Verknüpfung sich auf einen Abschnitt bezieht der allgemeine Information beinhaltet, machen Sie sich mit diesen Informationen vertraut und wechseln Sie zum nächsten Punkt aus der Liste.

	Aufgabe	Verknüpfung
☐	Ein oder mehrere Container erstellen	Container erstellen (auf Seite 61)
☐	Sicherungskopien der Containerschlüssel erstellen	Sicherungskopie der Containerschlüssel erstellen (auf Seite 70)
☐	Sicherungskopien der Konfiguration regelmäßig erstellen	Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen (auf Seite 112)
☐	Regelmäßig Exportdateien des Containers erstellen	Container exportieren (auf Seite 97)
☐	Vorbereitung zur Arbeit unter potentiell unsicheren Bedingungen	Vorbereitung für den Einsatz in einer unsicheren Umgebung: Vorgehensweise (auf Seite 134)
☐	Stets vollständige Bereinigung durchführen, um alle Spuren der Arbeit mit vertraulichen Daten zu beseitigen	Bereinigung von Datenspuren: Reihenfolge der Schritte (auf Seite 148)

Tipp. Es wird empfohlen, die Liste auszudrucken und die einzelnen Punkte nach ihrer Abarbeitung zu markieren.

Container erstellen

Der Assistent **Erstellen des Containers** startet automatisch beim ersten Start von ViPNet SafeDisk (s. ViPNet SafeDisk zum ersten Mal starten auf Seite 36) oder wenn im Programm noch kein Container erstellt wurde.

Wenn Sie die kostenlose Version von ViPNet SafeDisk nutzen, in der ein Container bereits erstellt wurde, erscheint eine Meldung über die eingeschränkte Funktionalität der kostenlosen Version.

Einschränkungen der unregistrierten Version von ViPNet SafeDisk
Sie haben eine Free Edition von ViPNet SafeDisk installiert. Um einen weiteren Container zu erstellen, kaufen und registrieren Sie bitte eine Vollversion von ViPNet SafeDisk.
Weitere Einschränkungen in der Free Edition?
ViPNet SafeDisk registrieren...

Abbildung 29: Meldung über die Einschränkungen in der kostenlosen Version

Um in der kostenlosen Version einen neuen Container zu erstellen, löschen Sie den bereits existierenden Container (s. Container löschen auf Seite 91) oder kaufen Sie die Vollversion (s. Registrierung von ViPNet SafeDisk auf Seite 41).

Zum Erstellen eines neuen Containers:

1. Führen Sie einen der folgenden Schritte durch:

   - Klicken Sie auf die Schaltfläche **Erstellen** in der Symbolleiste des Programms.
   - Wählen Sie im Menü **Container** den Befehl **Erstellen**.
   - Drücken Sie die Taste **Einfg**.

   Es wird der Assistent **Erstellen des Containers** gestartet.

2. Klicken Sie im Fenster **Erstellen des Containers** auf die Schaltfläche und geben den Pfad zur Datei des neuen Containers sowie seinen Namen an. Sie können auch die Standardwerte für Pfad und Dateinamen übernehmen.

Erstellen des Containers
Erstellen eines Containers
Dieser Assistent hilft Ihnen, einen Container zu erstellen, in dem Sie Ihre sensiblen Daten abspeichern können. Der Container wird in Form einer verschlüsselten Datei auf Ihrer Festplatte abgelegt.
Bestimmen Sie die Container-Datei:
C:\Users\Fortress\Documents\ContainerD0B2.sdc
...
Zum Fortfahren klicken Sie auf "Weiter".
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 30: Assistent „Erstellen des Containers“

Zum Fortfahren klicken Sie auf **Weiter**.

3 Auf der Seite **Container-Eigenschaften**:

- Geben Sie im Feld **Container-Größe** die Größe des neuen Containers an.
- Bei der Definition der Container-Größe gelten folgende Einschränkungen:
  - Die Größe des Containers muss in einem Bereich zwischen 1024 KB (1 MB) und 2048 GB liegen.
  - Wenn die Container-Größe weniger als 3 MB beträgt, kann der Container nicht mit dem NTFS-Dateisystem formatiert werden.
  - Wenn die Container-Größe mehr als 2048 MB (2 GB) beträgt, kann der Container nicht mit dem FAT-Dateisystem formatiert werden.
  - Wenn die Container-Größe weniger als 32 MB und mehr als 4095 MB (4 GB) beträgt, kann der Container nicht mit dem FAT32-Dateisystem formatiert werden.

Hinweis. Die Dateisystem des Containers kann später bei seiner Formatierung bestimmt werden. Es ist dennoch empfehlenswert, an dieser Stelle die optimale Größe zu definieren.

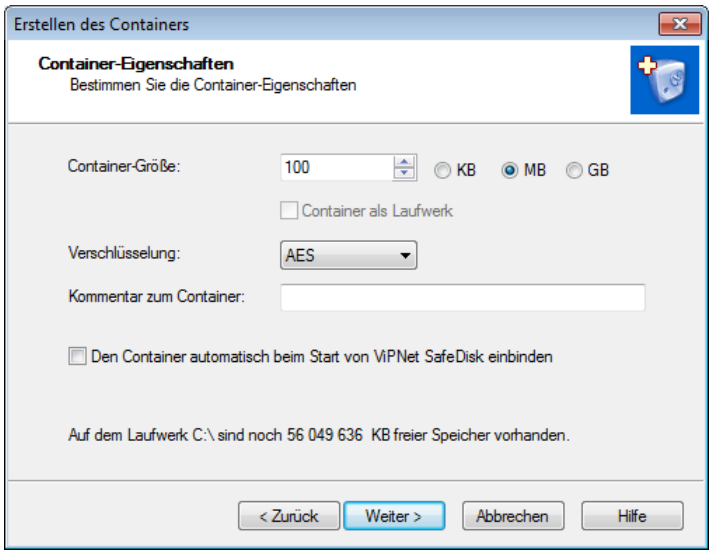

Abbildung 31: Container-Eigenschaften definieren

- Beim Erstellen des Containers auf einem externen Datenträger steht die Funktion zur Verfügung, den Container als ein vollständiges Laufwerk anzulegen. Wenn das Kontrollkästchen **Container als Laufwerk** aktiviert wird, dann ist die Angabe der Speichergröße für den zu erstellenden Container nicht mehr nötig. Die Größe des neuen Containers wird in diesem Fall dem Speichervolumen des externen Datenträgers entsprechen. Bei Verwendung dieser Funktion werden alle Daten, die auf dem externen Gerät gespeichert sind, unwiderbringlich gelöscht. Deswegen empfehlen wir Ihnen, rechtzeitig Sicherungskopien aller benötigten Daten zu erstellen und den Gerätespeicher vor dem Erstellen eines Containerlaufwerks zu leeren.
- Wählen Sie aus der Liste **Verschlüsselung** den Verschlüsselungsalgorithmus für diesen Container. Im Feld **Kommentar zum Container** können Sie einen beliebigen Kommentar eingeben. Dieser wird im Programmfenster von ViPNet SafeDisk rechts vom Containernamen abgebildet. Kurze, durchdachte Beschreibungen können dabei helfen, den benötigten Container schneller zu finden.
- Wenn Sie wollen, dass der Container automatisch beim Start von ViPNet SafeDisk eingebunden wird, aktivieren Sie das Kontrollkästchen **Den Container automatisch beim Start von ViPNet SafeDisk einbinden**.

Tipp. Wenn Sie das Kontrollkästchen **Den Container automatisch beim Start von ViPNet SafeDisk einbinden** nicht aktiviert haben, können Sie diese Einstellung später in den Container-Eigenschaften ändern.

Klicken Sie auf **Weiter**.

4 Auf der Seite **Zugriffstyp auf den Container** bestimmen Sie, welche Bestätigung beim Zugriff auf den Container verwendet wird.

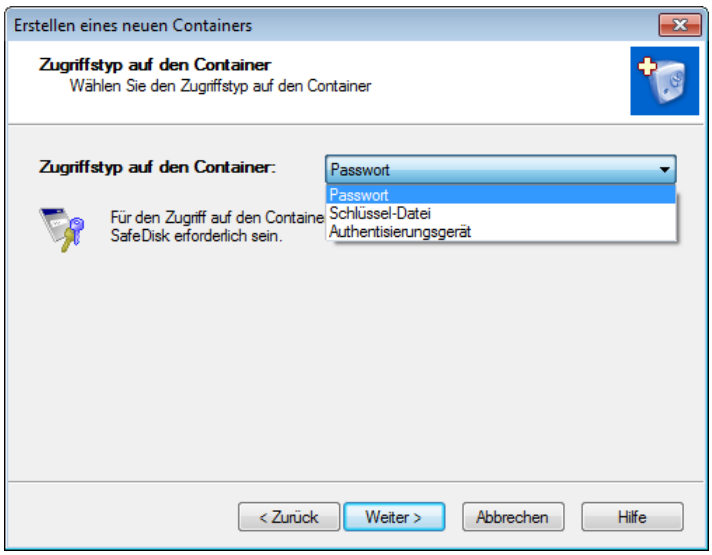

Abbildung 32: Zugriffstyp auf den Container

Sie können zwischen drei Zugriffstypen wählen:

- **Passwort**. Der Container ist durch das Passwort bei der Anmeldung in SafeDisk geschützt.
- **Schlüssel-Datei**. Der Container ist durch das Passwort bei der Anmeldung in SafeDisk sowie durch die Schlüssel-Datei geschützt. Bei der Auswahl dieses Zugriffstyps werden der Dateiname und der Pfad angegeben. Ohne Schlüssel-Datei ist der Zugriff auf den Container nicht möglich.

  Wenn Sie als Zugriffstyp Schlüssel-Datei gewählt haben, führen Sie die folgenden Schritte durch:

  - Klicken Sie auf und im Fenster **Erstellen der Schlüssel-Datei** definieren Sie den Ordner, in dem die Schlüssel-Datei gespeichert wird. Die Schlüssel-Datei kann beliebig benannt werden und kann eine beliebige Dateierweiterung haben.

Achtung! Es ist empfehlenswert, die Schlüssel-Datei auf einem externen Datenträger aufzubewahren, um den höheren Grad an Sicherheit zu gewährleisten.

Beachten Sie, dass im Fall des Verlustes der Schlüssel-Datei der Zugriff auf den Container für den sie bestimmt ist nicht mehr möglich ist.

Wenn die Schlüsseldatei beschädigt ist, kann der Zugriff auf den Container nur mit einer Sicherungskopie dieser Datei erfolgen. Aus diesem Grund ist es empfehlenswert, eine Sicherungskopie der Schlüssel-Datei für jeden Container zu erstellen. Mehr

---

darüber lesen im Abschnitt Sicherungskopie der Container-Schlüssel erstellen (s. Sicherungskopie der Containerschlüssel erstellen auf Seite 70).

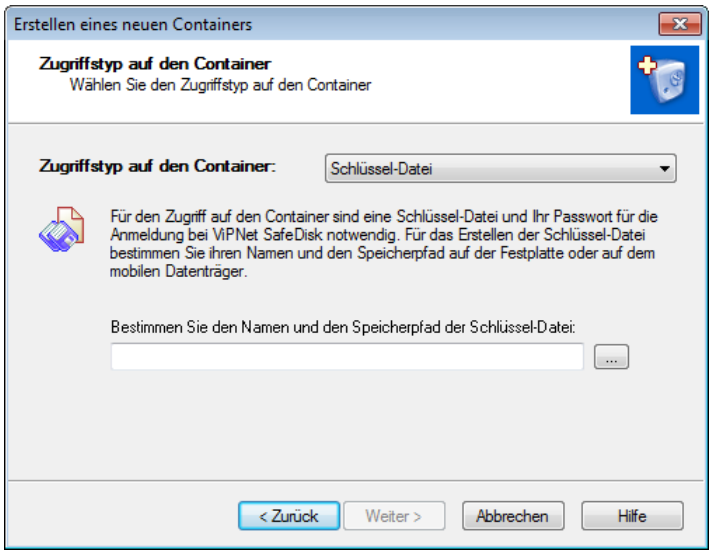
Erstellen eines neuen Containers
Zugriffstyp auf den Container
Wählen Sie den Zugriffstyp auf den Container
Zugriffstyp auf den Container:
Schlüssel-Datei
Für den Zugriff auf den Container sind eine Schlüssel-Datei und Ihr Passwort für die Anmeldung bei ViPNet SafeDisk notwendig. Für das Erstellen der Schlüssel-Datei bestimmen Sie ihren Namen und den Speicherpfad auf der Festplatte oder auf dem mobilen Datenträger.
Bestimmen Sie den Namen und den Speicherpfad der Schlüssel-Datei:
...
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 33: Schlüssel-Datei für den Container bestimmen

- **Authentisierungsgerät**. Der Container ist durch das Passwort bei der Anmeldung in SafeDisk sowie durch das Authentisierungsgerät geschützt. Um den Zugriff auf den Container zu gewährleisten, muss das Authentisierungsgerät angeschlossen sein.

  Wenn Sie als Zugriffstyp Authentisierungsgerät gewählt haben, führen Sie die folgenden Schritte durch:

  - Schleißen Sie das Authentisierungsgerät an.
  - In der Dropdown-Liste **Wählen Sie das Authentisierungsgerät** wählen Sie den Typ Ihres Authentisierungsgeräts.

Hinweis. Auf Ihrem Computer sollte der Treiber des externen Geräts sowie alle weiteren benötigten Programme installiert sein. Wenn Ihr Authentisierungsgerät nicht in der Dropdown-Liste **Wählen Sie das Authentisierungsgerät** vorhanden ist, ist er nicht korrekt installiert.

Die Angaben zur Treiber-Installation finden Sie im Benutzerhandbuch Ihres Authentisierungsgeräts. Mehr Informationen finden Sie im Abschnitt Externe Datenträger (auf Seite 171).

  - Im Feld **Geben Sie die PIN ein** geben Sie die PIN Ihres Authentisierungsgeräts ein.

- Wenn Sie die PIN nicht bei jedem Einbinden des Containers eingeben wollen, aktivieren Sie die Option **PIN speichern**.

Hinweis. Die Eingabe der PIN bei jedem Einbinden des Containers gewährleistet besseren Schutz Ihrer Daten. Deshalb ist es empfehlenswert die Option **PIN speichern** nicht zu aktivieren

Die Angaben über das Definieren von PIN sowie über die anderen Einstellungen finden Sie im Benutzerhandbuch Ihres Authentisierungsgeräts.

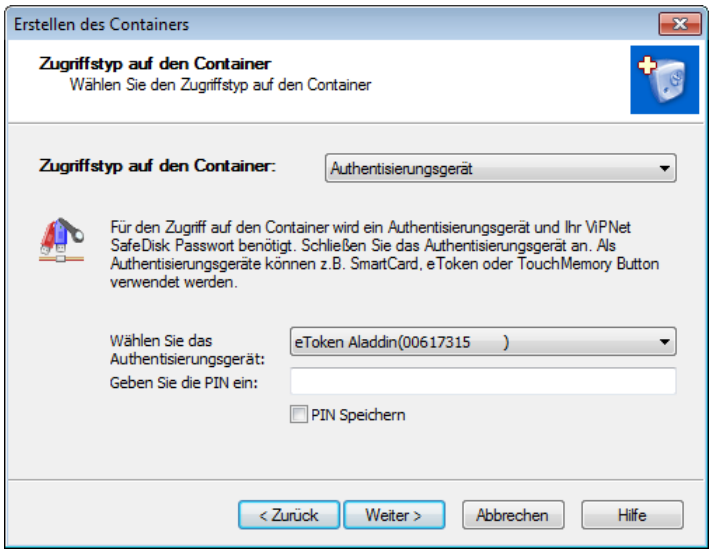
Erstellen des Containers
Zugriffstyp auf den Container
Wählen Sie den Zugriffstyp auf den Container
Zugriffstyp auf den Container:
Authentisierungsgerät
Für den Zugriff auf den Container wird ein Authentisierungsgerät und Ihr ViPNet SafeDisk Passwort benötigt. Schließen Sie das Authentisierungsgerät an. Als Authentisierungsgeräte können z.B. SmartCard, eToken oder TouchMemory Button verwendet werden.
Wählen Sie das Authentisierungsgerät:
eToken Aladdin(00617315)
Geben Sie die PIN ein:
PIN Speichern
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 34: Zugriffstyp auf den Container

Achtung! Wenn beim Erstellen des Containers unter Verwendung des Zugriffstyps **Authentisierungsgerät** der Fehler „Container konnte nicht erstellt werden“ eingeblendet wird, dann kann die Ursache darin liegen, dass nicht genügend Speicherplatz auf dem externen Gerät zur Verfügung steht. Falls dieser Fehler auftaucht, folgen Sie den Empfehlungen, die im Abschnitt Container mit Zugriffstyp „Authentisierungsgerät“ konnte nicht erstellt werden (auf Seite 167) aufgeführt sind.

---

5 Klicken Sie auf **Weiter**. Es wird das digitale Roulette gestartet (falls es nicht bereits früher während der laufenden Arbeitssitzung von ViPNet SafeDisk gestartet wurde).

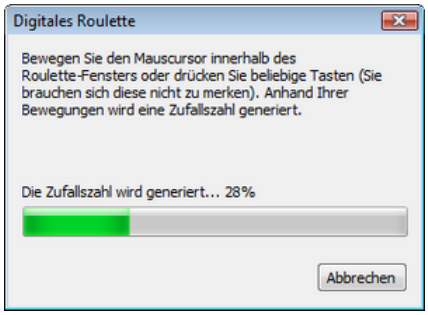
Digitales Roulette
Bewegen Sie den Mauscursor innerhalb des Roulette-Fensters oder drücken Sie beliebige Tasten (Sie brauchen sich diese nicht zu merken). Anhand Ihrer Bewegungen wird eine Zufallszahl generiert.
Die Zufallszahl wird generiert... 28%
Abbrechen

Abbildung 35: Digitales Roulette

Folgen Sie den Anweisungen im Fenster **Digitales Roulette**. Auf diese Weise werden die Schlüssel des Containers erstellt.

6 Klicken Sie auf der Seite **Abschluss der Erstellung des Containers** auf die Schaltfläche **Fertig**. Wenn das Kontrollkästchen **Erstellung einer Sicherungskopie der Containerschlüssel starten** aktiviert ist, wird anschließend automatisch der Assistent **Erstellen der Sicherungskopie der Containerschlüssel** gestartet (s. Sicherungskopie der Containerschlüssel erstellen auf Seite 70).

Wenn dieses Kontrollkästchen deaktiviert wurde, bindet das Programm den neu erstellten Container automatisch ein und schlägt seine Formatierung vor.

Erstellen des Containers
Abschluss der Erstellung des Containers
Achtung! Zusammen mit dem Container wurden Schlüssel erstellt, durch die die Verschlüsselung des Containers erfolgt. Nach dem Beenden des Assistenten muss eine Sicherungskopie der Containerschlüssel erstellt werden. Sie ermöglicht das Wiederherstellen der Schlüssel und des Zugriffs auf den Container nach möglichen Störungen.
Erstellung einer Sicherungskopie der Containerschlüssel starten
Fertig

Abbildung 36: Abschluss der Erstellung des Containers

Dadurch wird im von Ihnen angegebenen Ordner die versteckte Container-Datei *.sdc (s. Container-Datei auf Seite 179) erzeugt. Zum Anzeigen dieser Datei öffnen Sie in der Systemsteuerung das Fenster **Ordner- und Suchoptionen** und aktivieren Sie auf der Registerkarte **Ansicht** die entsprechende Option unter dem Eintrag **Versteckte Dateien und Ordner**.

Achtung! In der aktuellen Version des Programms kann die Datei mit Komprimierungs- und Verschlüsselungsattributen nicht als -Container benutzt werden.

Sicherungskopie der Container-Schlüssel

Eine Sicherungskopie der Containerschlüssel kann in folgenden Fällen erforderlich sein:

- Sie erhalten keinen Zugang zum Container, obwohl die Container-Datei nicht beschädigt ist;
- Die Schlüssel-Datei für den Container ist beschädigt;
- nach der Konvertierung in das neue Format können Sie auf Container, die in früheren Versionen von ViPNet SafeDisk erstellt wurden, nicht mehr zugreifen;
- nach dem Schlüsselupdate können Sie auf den Container nicht mehr zugreifen;
- Sie wollen den Containerzugang für einen anderen Benutzer, der auf Ihrem Computer registriert ist, ermöglichen;
- Sie wollen die Container-Datei *.sdc manuell kopieren (ohne Verwendung der Export-Funktionalität des Containers).

Achtung! Sie können die Sicherungskopie der Containerschlüssel für die Wiederherstellung des Zugangs zu geschützten Daten verwenden, wenn die Containerschlüssel beschädigt wurden. Wenn die Container-Datei selbst beschädigt wurde, können die darin enthaltenen Daten nur durch einen Import der Container-Datei wiederhergestellt werden (wenn zu einem früheren Zeitpunkt eine Exportdatei dieses Containers erstellt wurde).

Deswegen wird ausdrücklich empfohlen, regelmäßig vollständige Sicherungskopien aller Container zu erstellen (s. Container exportieren auf Seite 97).

Assistenten zur Erstellung von Sicherungskopien der Containerschlüssel starten

Wenn Sie eine Sicherungskopie der Schlüssel für einen Container erstellen möchten, der bereits existiert, führen Sie zum Starten des Assistenten **Erstellen der Sicherungskopie der Containerschlüssel** die folgenden Schritte aus:

1. Wählen Sie im Programmfenster von ViPNet SafeDisk den Container aus, für welchen eine Sicherungskopie der Schlüssel erstellt werden soll.
2. Wenn der Container eingebunden ist, trennen Sie ihn.
3. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie im Menü **Container** den Eintrag **Sicherungskopie der Containerschlüssel**.
   - Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Eintrag **Sicherungskopie der Schlüssel**.

   Es wird der Assistent **Erstellen der Sicherungskopie der Containerschlüssel** gestartet.

Sicherungskopie der Containerschlüssel erstellen

1. Klicken Sie auf der ersten Seite des Assistenten **Erstellen der Sicherungskopie der Containerschlüssel** (s. Sicherungskopie der Containerschlüssel auf Seite 180) auf **Weiter**.
2. Auf der Seite **Art der Speicherung der Sicherungskopie der Containerschlüssel** gehen Sie wie folgt vor:

- Wenn Sie die Sicherungskopie in einer Datei auf dem Computer speichern wollen, wählen Sie in der Liste **Art der Speicherung** den Eintrag **Datei** aus.

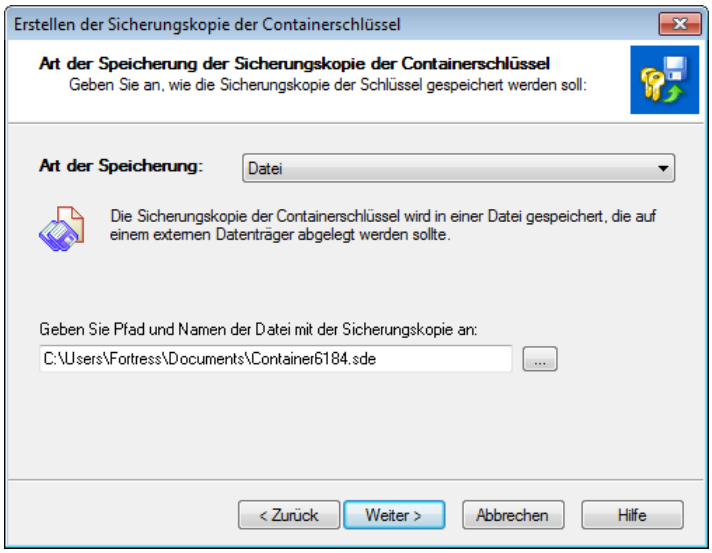
Erstellen der Sicherungskopie der Containerschlüssel
Art der Speicherung der Sicherungskopie der Containerschlüssel
Geben Sie an, wie die Sicherungskopie der Schlüssel gespeichert werden soll:
Art der Speicherung:
Datei
Die Sicherungskopie der Containerschlüssel wird in einer Datei gespeichert, die auf einem externen Datenträger abgelegt werden sollte.
Geben Sie Pfad und Namen der Datei mit der Sicherungskopie an:
C:\Users\Fortress\Documents\Container6184.sde
...
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 37: Sicherungskopie der Schlüssel in einer Datei speichern

Klicken Sie auf und geben Sie den Ordner an, in welchem Sie die Sicherungskopie der Schlüssel speichern wollen. Sie können auch den standardmäßig vorgeschlagenen Ordner übernehmen. Klicken Sie anschließend auf **Weiter**.

Tipp. Speichern Sie die Sicherungskopie der Containerschlüssel aus Sicherheitsgründen nicht in demselben Ordner ab, in dem sich die Container-Datei befindet. Wir empfehlen Ihnen, abnehmbares Gerät zum Speichern der Sicherungskopie der Containerschlüssel zu nutzen.

- Wenn Sie die Sicherungskopie auf einem Authentisierungsgerät speichern wollen:
  - Wählen Sie in der Liste **Art der Speicherung** den Eintrag **Authentisierungsgerät** aus.
  - Geben Sie im Feld **Name der Sicherungskopie der Schlüssel** den Namen der Sicherungskopie ein.
  - Stellen Sie sicher, dass das Authentisierungsgerät mit der entsprechenden Leseeinrichtung verbunden ist.
  - Wählen Sie in der Liste **Gerät** das verwendete Authentisierungsgerät aus (wenn es nicht bereits automatisch ausgewählt wurde).

- Geben Sie im Feld **Geben Sie die PIN ein** die PIN für das Authentisierungsgerät ein. Um die PIN zu speichern, aktivieren Sie das entsprechende Kontrollkästchen.
- Klicken Sie auf **Weiter**.

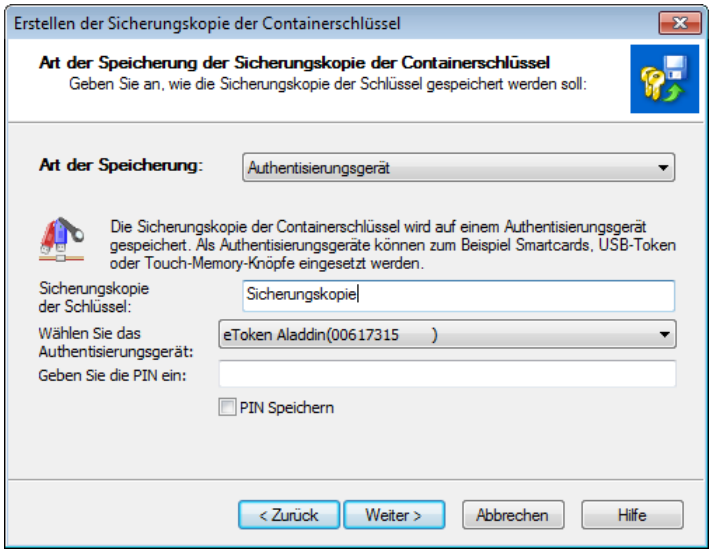
Erstellen der Sicherungskopie der Containerschlüssel
Art der Speicherung der Sicherungskopie der Containerschlüssel
Geben Sie an, wie die Sicherungskopie der Schlüssel gespeichert werden soll:
Art der Speicherung:
Authentisierungsgerät
Die Sicherungskopie der Containerschlüssel wird auf einem Authentisierungsgerät gespeichert. Als Authentisierungsgeräte können zum Beispiel Smartcards, USB-Token oder Touch-Memory-Knöpfe eingesetzt werden.
Sicherungskopie der Schlüssel:
Sicherungskopie
Wählen Sie das Authentisierungsgerät:
eToken Aladdin(00617315)
Geben Sie die PIN ein:
PIN Speichern
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 38: Sicherungskopie auf einem Authentisierungsgerät speichern

3 Geben Sie auf der Seite **Zugangspasswort** das Kennwort für die Sicherungskopie ein und wiederholen zur Bestätigung die Eingabe. Klicken Sie auf **Weiter**.

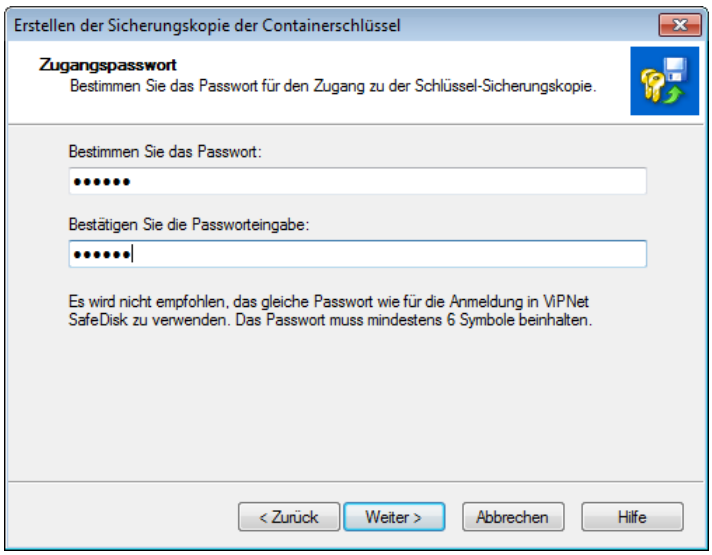
Erstellen der Sicherungskopie der Containerschlüssel
Zugangspasswort
Bestimmen Sie das Passwort für den Zugang zu der Schlüssel-Sicherungskopie.
Bestimmen Sie das Passwort:
Bestätigen Sie die Passworteingabe:
Es wird nicht empfohlen, das gleiche Passwort wie für die Anmeldung in ViPNet SafeDisk zu verwenden. Das Passwort muss mindestens 6 Symbole beinhalten.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 39: Kennwort für den Zugang zur Sicherungskopie der Containerschlüssel einrichten

4 Klicken Sie auf der Seite **Abschluss der Erstellung der Sicherungskopie der Containerschlüssel** auf **Fertig**.

Es wird entweder eine Datei mit der Erweiterung SDE erstellt, die die Sicherungskopie der Containerschlüssel enthält oder die Sicherungskopie der Containerschlüssel wird auf dem Authentisierungsgerät abgelegt.

Container einbinden

Nachdem Sie einen neuen Container erstellt haben und die Sicherungskopie der Container-Schlüssel generiert haben können Sie den Container einbinden um dort Ihre Daten speichern zu können.

Für die Einbindung eines bereits existierenden Containers z.B. nach dem Neustart von ViPNet SafeDisk, siehe Einen früher erstellen Container einbinden (auf Seite 77).

Um den neuen Container einzubinden:

1 Führen Sie die folgenden Schritte durch:

- Im Fenster **Einbinden des Containers** klicken Sie auf **Ja**.

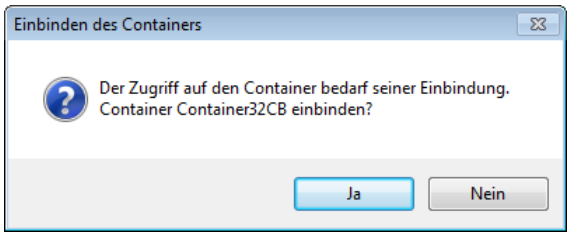

Abbildung 40: Vorschlag zur Einbindung des Containers

- Wählen Sie im Hauptfenster des Programs ViPNet SafeDisk den Container, der Sie einbinden wollen, und führen eine der folgenden Schritte durch:

  - Klicken Sie in der Szmbolleiste auf **Einbinden** .
  - Wählen Sie im Menü **Container** den Punkt **Einbinden**.
  - Klicken Sie auf den **Container** mit der rechten Maustaste und wählen den Punkt **Einbinden** im Kontextmenü.
  - Drücken Sie auf die Taste **C**.

2 Im Fenster **Container einbinden als Laufwerk** führen Sie die folgenden Schritte durch:

- In der Liste **Container einbinden als Laufwerk** wählen Sie den Laufwerksbuchstaben, welcher dem Container unter Windows entsprechen soll.

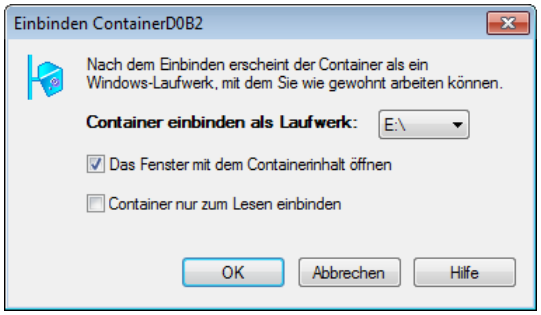
Einbinden ContainerD0B2
Nach dem Einbinden erscheint der Container als ein Windows-Laufwerk, mit dem Sie wie gewohnt arbeiten können.
Container einbinden als Laufwerk:
E:\
Das Fenster mit dem Containerinhalt öffnen
Container nur zum Lesen einbinden
OK
Abbrechen
Hilfe

Abbildung 41: Container einbinden

- Wenn Sie den Container sofort öffnen wollen, aktivieren Sie die Option **Das Fenster mit dem Containerhalt öffnen**.
- Wenn Sie nicht wollen, dass der Inhalt des Containers nach diesem Start geändert wird, aktivieren Sie die Option **Container nur zum Lesen einbinden.**

Hinweis. Wenn Sie einen neuen Container erstellen, soll die Option **Container nur zum Lesen einbinden** deaktiviert bleiben, um den Container formatieren zu können. Wenn Sie die Option aktiviert haben, trennen Sie den Container und binden Sie ihn erneut ein oder erstellen Sie den Container neu, ohne die Option zu aktivieren.

- Wenn Sie unter Windows XP oder Windows Server 2003 arbeiten und möchten, dass niemand außer Ihnen Zugang zum Container besitzt, dann aktivieren Sie das Kontrollkästchen **Exklusiver Zugriff**.

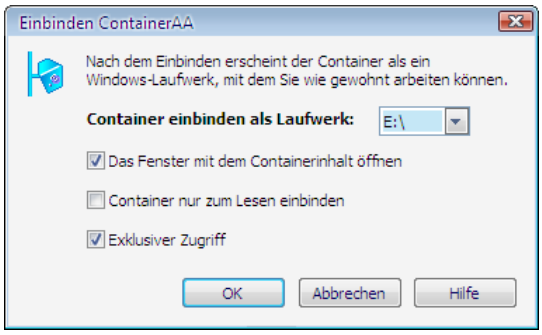

Abbildung 42: Exklusiver Zugriff aktivieren

Hinweis. Beim Verwenden der Option **Exklusiver Zugriff** kann der Container nicht ausschließlich zum Lesen eingebunden werden.

3 Klicken Sie auf **OK**.

4 Wenn Sie einen neuen Container einbinden, erscheint eine Meldung mit der Aufforderung, den Container zu formatieren.

Container einbinden, der durch eine Schlüssel-Datei geschützt ist

1 Im Fenster **Einbinden des Containers** (s. Abbildung auf Seite 74) klicken Sie auf **Ja**.

2 Wenn der Speicherort der Schlüssel-Datei sich nach dem letzten Start geändert hat, öffnet sich das Fenster **Schlüssel-Datei des Containers**.

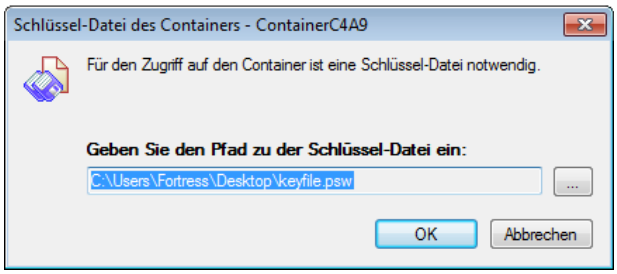

Abbildung 43: Pfad zu der Schlüssel-Datei eingeben

Klicken Sie auf die Taste ... und definieren Sie den Pfad zu der Schlüssel-Datei. Klicken Sie anschließend auf **OK**.

Wenn der Speicherort der Schlüssel-Datei sich nicht verändert hat, wird sich das Fenster **Schlüssel-Datei des Containers** nicht öffnen.

Hinweis. Wenn die Schlüssel-Datei des Containers durch Hardwarefehler oder durch einen Angriff beschädigt wurde, kann der Zugriff auf den Container nur mit Hilfe einer Sicherungskopie der Schlüssel-Datei mit anschließendem Import des Containers wiederhergestellt werden (s. Sicherungskopie der Containerschlüssel erstellen auf Seite 70).

3 Im Fenster **Container einbinden als Laufwerk** (s. Abbildung auf Seite 75) definieren Sie die Eigenschaften des Containers beim Einbinden und klicken Sie auf **OK**.

4 Wenn Sie einen neuen Container einbinden, erscheint eine Meldung über die Formatierung des Containers.

Container einbinden, der durch eine Authentisierungsgeräti geschützt ist

1 Im Fenster **Einbinden des Containers** (s. Abbildung auf Seite 74) klicken Sie auf **Ja**.

2 Schließen Sie das Authentisierungsgerät an, das Sie bei der Erstellung des Containers verwendet haben.

3 Im Fenster **Authentisierungsgerät des Containers** im Feld **Geben Sie die PIN ein** geben Sie die PIN des Authentisierungsgeräts ein und klicken Sie auf **OK**.

Hinweis. Es ist empfehlenswert die Option **PIN speichern zu** deaktivieren, um besseren Schutz zu gewährleisten.

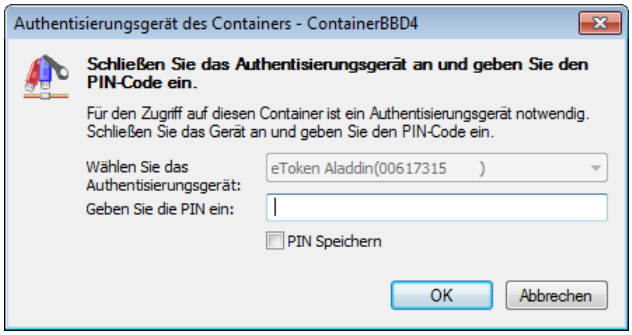
Authentisierungsgerät des Containers - ContainerBBD4
Schließen Sie das Authentisierungsgerät an und geben Sie den PIN-Code ein.
Für den Zugriff auf diesen Container ist ein Authentisierungsgerät notwendig. Schließen Sie das Gerät an und geben Sie den PIN-Code ein.
Wählen Sie das Authentisierungsgerät:
eToken Aladdin(00617315)
Geben Sie die PIN ein:
PIN Speichern
OK
Abbrechen

Abbildung 44: PIN des Authentisierungsgeräts eingeben

4 Im Fenster **Container einbinden als Laufwerk** (s. Abbildung auf Seite 75) definieren Sie die Eigenschaften des Containers beim Einbinden und klicken Sie auf **OK**.

5 Wenn Sie einen neuen Container einbinden, erscheint eine Meldung über die Formatierung des Containers.

Einen früher erstellen Container einbinden

Zum Einbinden eines früher angelegten Containers gehen Sie wie folgt vor:

1 Wählen Sie im Programmfenster von ViPNet SafeDisk den Container aus, der eingebunden werden soll.

2 Führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Einbinden** .
- Wählen Sie im Menü **Container** den Befehl **Einbinden**.
- Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Befehl **Einbinden**.
- Drücken Sie die Taste **C**.

3 Abhängig davon, wie der Container geschützt ist, führen Sie einen der folgenden Schritte durch:

- Wenn der Container durch das Passwort geschützt ist, wechseln Sie zum Schritt 4.
- Wenn der Container durch Schlüssel-Datei geschützt ist und die Datei nicht automatisch gefunden wurde definieren Sie den Pfad zu der Datei (s. Container einbinden, der durch eine Schlüssel-Datei geschützt ist auf Seite 76).
- Wenn der Container durch ein Authentisierungsgerät geschützt ist (s. Container einbinden, der durch eine Authentisierungsgeräti geschützt ist auf Seite 77), schließen Sie das Gerät an.

4 Im Fenster **Container einbinden als Laufwerk** (s. Abbildung auf Seite 75) definieren Sie die Eigenschaften des Containers beim Einbinden und klicken Sie auf **OK**.

5 Jetzt können Sie Ihre Daten im Container schützen.

Container formatieren

Vor Beginn der Nutzung muss ein Container formatiert werden. Bei Einbindung eines nicht formatierten Containers wird automatisch der Assistent **Container formatieren** gestartet. Zum Formatieren eines Containers:

1 Wählen Sie auf der ersten Seite des Assistenten in der Liste Dateisystem das richtige Dateisystem für die Formatierung aus.

Hinweis. Die Wahl des Dateisystems hängt von der Containergröße ab:

- Das Dateisystem FAT kann ausgewählt werden, falls die Containergröße mehr als 1 MB und weniger als 2 GB beträgt.
- Das Dateisystem FAT32 kann ausgewählt werden, falls die Containergröße mehr als 32 MB und weniger als 8 GB beträgt.
- Das Dateisystem NTFS kann ausgewählt werden, falls die Containergröße mehr als 3 MB beträgt.

Container formatieren
Container formatieren
Damit der Container benutzt werden kann, muss er formatiert werden. Dieser Vorgang kann einige Minuten in Anspruch nehmen.
Container: Container32CB
Dateisystem: NTFS
Klicken Sie auf "Weiter", um die Formatierung zu starten. Der Vorgang der Formatierung kann später nicht mehr unterbrochen werden.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 45: Assistent für die Container-Formatierung

2 Klicken Sie auf **Weiter**, um mit der Formatierung zu beginnen.

Hinweis. Der Vorgang der Formatierung kann einige Minuten oder einge Stunden dauern, abhängig von der Containergröße und der Computerleistung.

3 Nach Abschluss der Formatierung klicken Sie auf der letzten Seite des Assistenten auf die Schaltfläche **Fertig**. Der Container ist nun einsatzbereit.

Tägliche Arbeit mit den geschützten Daten

Nach der Erstellung aller Container können Sie Ihre Daten im Container schützen. Folgende Vorgehensweise ist dabei empfehlenswert:

1. Starten Sie ViPNet SafeDisk (s. ViPNet SafeDisk starten auf Seite 29).
2. Wählen Sie im Programmfenster von ViPNet SafeDisk den Container aus, der die benötigten Daten enthält.
3. Klicken Sie auf **Einbinden** , um den Container einzubinden. Es wird das Fenster **Einbinden** (s. Abbildung auf Seite 75) eingeblendet. Geben Sie die Parameter für die Einbindung an und klicken auf **OK**.

   Mehr über das Einbinden des Containers s. Kapitel Container einbinden.
4. Doppelklicken Sie auf den eingebundenen Container. In einem separaten Fenster wird das Container-Laufwerk angezeigt. Sie können nun mit dem Container wie mit einem gewöhnlichen Windows-Laufwerk arbeiten: Daten, die Sie schützen möchten, dort abspeichern oder Dokumente auf dem Laufwerk ablegen und editieren.

Hinweis. Bevor Sie anfangen, mit dem Container zu arbeiten, lesen Sie den Abschnitt Abgrenzung des Containerzugangs (auf Seite 122).

5. Wenn Sie die Arbeit mit geschützten Daten beenden wollen, schließen Sie zunächst alle Dateien, die im Container enthalten sind, sowie alle Fenster, die den Containerinhalt abbilden. Wählen Sie anschließend im Programmfenster den benötigten Container aus und klicken Sie auf die Schaltfläche **Trennen** . Nach dem Trennen des Containers ist der Zugang zu geschützten Daten nicht mehr möglich, und die Präsenz dieser Daten auf dem Rechner ist nicht mehr offensichtlich.
6. Melden Sie sich in ViPNet SafeDisk ab (s. ViPNet SafeDisk beenden auf Seite 30).

Containersymbole in ViPNet SafeDisk

In der nachfolgenden Tabelle sind die Containersymbole von ViPNet SafeDisk samt ihrer Beschreibung aufgelistet.

Tabelle 3. Beschreibung der Containersymbole von

Containersymbol in	Symbolbeschreibung
	Container ist bereit, aber nicht eingebunden.
	Container ist bereit und eingebunden. Er kann wie ein gewöhnliches Windows-Laufwerk verwendet werden.
	Container ist erstellt, aber gegenwärtig nicht verfügbar (möglicherweise wurde die Container-Datei auf einem abnehmbaren Datenträger angelegt, zu dem nun kein Zugang besteht).
	Container ist beschädigt, da entweder die Container-Datei selbst oder die Containerschlüssel beschädigt sind. Ausführliche Informationen dazu finden Sie in Kapitel Wiederherstellen des Zugriffs auf die geschützten Daten (auf Seite 108).

Container trennen

Damit Ihre privaten Daten verborgen bleiben, sollten die Container getrennt werden. Außerdem können einige Aktionen nur mit getrennten Containern durchgeführt werden, zum Beispiel die Änderung der Container-Eigenschaften, der Export des Containers oder die Erstellung einer Sicherungskopie der Containerschlüssel.

Zum Trennen des Containers:

1. Wählen Sie im Hauptfenster den Container aus, der getrennt werden soll. Eingebundene Container werden durch das Symbol gekennzeichnet, getrennte durch das Symbol .

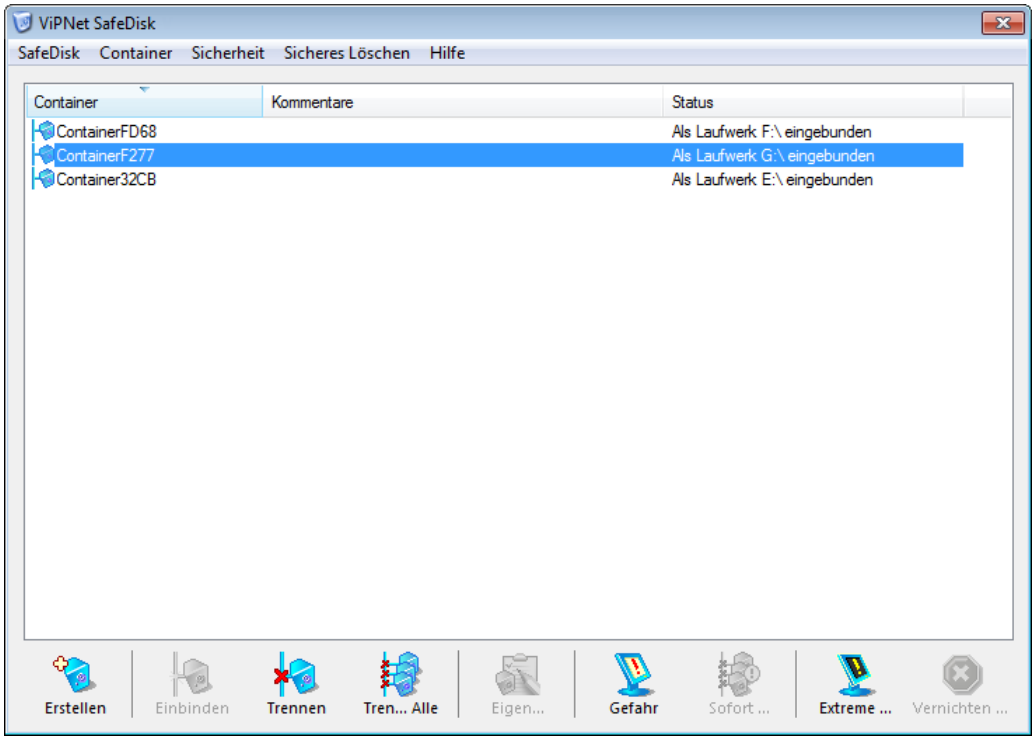

Abbildung 46: Eingebundene und getrennte Container

2. Schließen Sie alle Dateien, die im Container gespeichert sind, sowie alle Fenster, die den Containerinhalt abbilden.

3. Führen Sie im Programmfenster von ViPNet SafeDisk einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Trennen** .
- Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Befehl **Trennen**.
- Wählen Sie im Menü Container den Befehl **Trennen**.
- Drücken Sie die Taste **D**.

Wenn Sie alle Container gleichzeitig trennen wollen, führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Alle trennen** .
- Wählen Sie im Menü Container den Befehl **Alle trennen**.
- Drücken Sie die Tastenkombination **Alt+D**.

4 Wenn der Container aus irgendwelchen Gründen nicht getrennt werden kann (zum Beispiel wenn die im Container enthaltenen Dateien von anderen Anwendungen benutzt werden), wird vom Programm eine entsprechende Warnung ausgegeben.

Damit der Container zwangsweise getrennt wird, aktivieren Sie im Meldungsfenster das Kontrollkästchen **Zwangsweise Trennung veranlassen** und klicken Sie auf **Wiederholen**.

Achtung! Bei einer zwangsweisen Trennung des Containers werden geöffnete Dokumente nicht geschlossen. Diese Dokumente sollten Sie eigenhändig schließen.

Tipp. Damit beim Näherkommen Unbefugter alle Container sofort getrennt werden können, aktivieren Sie den „Gefahr“-Modus (s. Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus auf Seite 136).

Containereigenschaften ansehen und ändern

Führen Sie die folgenden Schritte aus, um Container-Eigenschaften anzuzeigen und (oder) zu ändern:

1. Wählen Sie im Hauptfenster von ViPNet SafeDisk den passenden Container aus und trennen ihn.
2. Führen Sie einen der nachfolgenden Schritte aus:
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Eigenschaften** .
   - Wählen Sie im Menü **Container** den Befehl **Eigenschaften**.
   - Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Eintrag **Eigenschaften**.
   - Drücken Sie die Tastenkombination **Alt+Eingabe**.
3. Im Fenster **Eigenschaften** können Sie in der Registerkarte **Container** die wichtigsten Parameter des gewählten Containers ändern:
   - Namen und Pfad des Containers (s. Container-Datei verschieben auf Seite 90);
   - Kommentar zum Container;
   - Das Kontrollkästchen **Den Container automatisch beim Start von ViPNet SafeDisk einbinden** aktivieren oder deaktivieren;
   - Das Kontrollkästchen **Nur zum Lesen einbinden**.

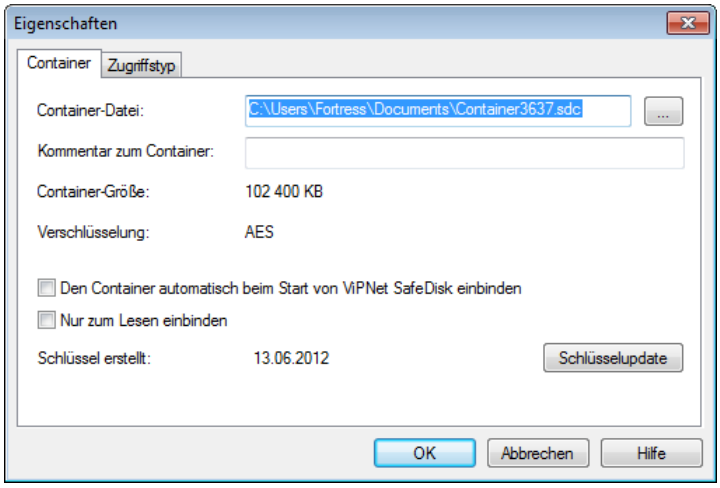

Abbildung 47: Containereigenschaften

In der Registerkarte **Container** können Sie das Erstellungsdatum der Containerschlüssel herausfinden und, wenn nötig, die Schlüssel aktualisieren (s. Containerschlüssel aktualisieren auf Seite 88), indem Sie auf die Schaltfläche **Schlüsselupdate** klicken.

Hinweis. Container-Größe und Verschlüsselungsalgorithmus können nicht geändert werden.

4 In der Registerkarte **Zugriffstyp** können Sie den Zugriffstyp auf den Container ändern.

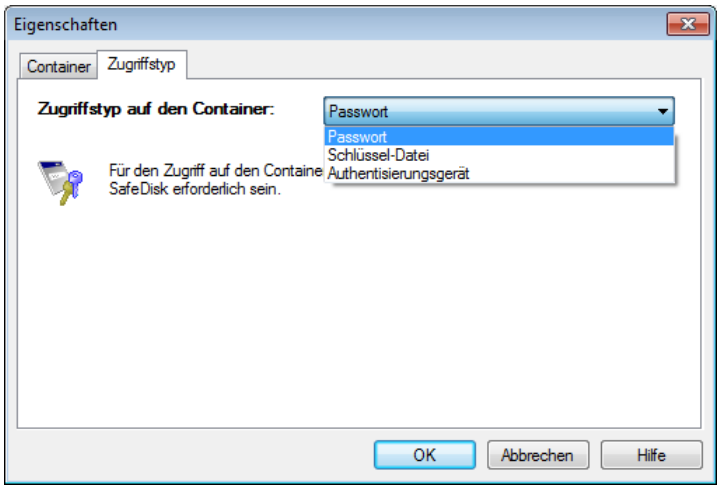

Abbildung 48: Auswahl des Zugriffstyps

Um den Zugriffstyp zu ändern, wählen Sie aus der Dropdown-Liste **Zugriffstyp auf den Container** eine der folgenden Optionen:

- **Passwort**. Für den Zugriff auf den Container ist es ausreichend, bei der Anmeldung in ViPNet SafeDisk das Passwort einzugeben.
- **Schlüssel-Datei**. Für die Anmeldung in ViPNet SafeDisk benötigen Sie ein Passwort und für den Zugriff auf den Container eine Schlüssel-Datei.

  Wenn Sie diesen Zugriffstyp gewählt haben, definieren Sie den Pfad und den Namen der Schlüssel-Datei.

Achtung! Es ist empfehlenswert, die Schlüssel-Datei auf einem externen Datenträger aufzubewahren, um einen höheren Grad an Sicherheit zu gewährleisten.

- **Authentisierungsgerät**. Für die Anmeldung in ViPNet SafeDisk benötigen Sie ein Passwort und für den Zugriff auf den Container das Authentisierungsgerät. Außerdem erfolgt der Zugriff auf einige Authentisierungsgeräte erst nach Eingabe einer PIN.

  Wenn Sie diesen Zugriffstyp gewählt haben, schließen Sie das Authentisierungsgerät an. Aus der Dropdown-Liste **Wählen Sie den Authentisierungsgerät** wählen Sie Ihr Authentisierungsgerät aus und im Feld **Geben Sie die PIN ein** geben Sie die PIN des Geräts ein.

Hinweis. Das Programm ViPNet SafeDisk unterstützt mehrere Typen von Authentisierungsgeräten. Ausführliche Informationen überAuthentisierungsgeräte s. Abschnitt Externe Datenträger (auf Seite 171).

5 Nachdem Sie die Änderungen vorgenommen haben klicken Sie auf **OK**, um die neuen Einstellungen zu speichern. Wenn Sie die neuen Einstellungen nicht speichern wollen klicken Sie auf **Abbrechen**.

Containerschlüssel aktualisieren

Damit die Sicherheit beim Schutz von Daten, die in -Containern gespeichert sind, erhöht werden kann, besteht die Möglichkeit zum Aktualisieren der Containerschlüssel (d. h. Schlüssel, mit denen die im Container enthaltenen Daten verschlüsselt werden). Nach dem Update wird der Zugang zum Container mit Hilfe alter Schlüssel (oder einer Sicherungskopie der alten Schlüssel) nicht mehr möglich sein. Es wird empfohlen, das Update der Containerschlüssel nicht seltener als alle 15 Monate durchzuführen. Das Erstellungsdatum der Containerschlüssel wird im Fenster **Eigenschaften** (s. Abbildung auf Seite 86) in der Registerkarte **Container** angezeigt.

Zum Aktualisieren des Containerschlüssels:

1. Wählen Sie im Programmfenster von ViPNet SafeDisk den Container aus, für welchen die Schlüssel aktualisiert werden sollen.
2. Führen Sie einen der folgenden Schritte durch:
   - Wählen Sie im Menü **Container** den Befehl **Schlüssel aktualisieren**.
   - Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Eintrag **Schlüsselupdate**.

     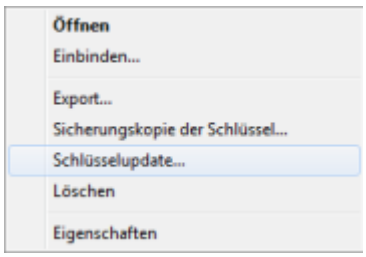

     Abbildung 49: Containerschlüsselupdate

   - Klicken Sie im Fenster **Eigenschaften** (s. Abbildung auf Seite 86) in der Registerkarte **Container** auf die Schaltfläche **Schlüsselupdate**.

   Es wird der Assistent **Containerschlüssel aktualisieren** gestartet.
3. Klicken Sie auf der ersten Seite des Assistenten **Containerschlüssel aktualisieren** auf die Schaltfläche **Weiter**.

   Es wird eine Seite mit der Fortschrittsanzeige des Update-Vorgangs eingeblendet. Sie können auf **Stopp** klicken, um den Vorgang zu anzuhalten.

4 Nach Abschluss der Schlüsselaktualisierung wird die Seite **Aktualisierung der Containerschlüssel wird abgeschlossen** eingeblendet.

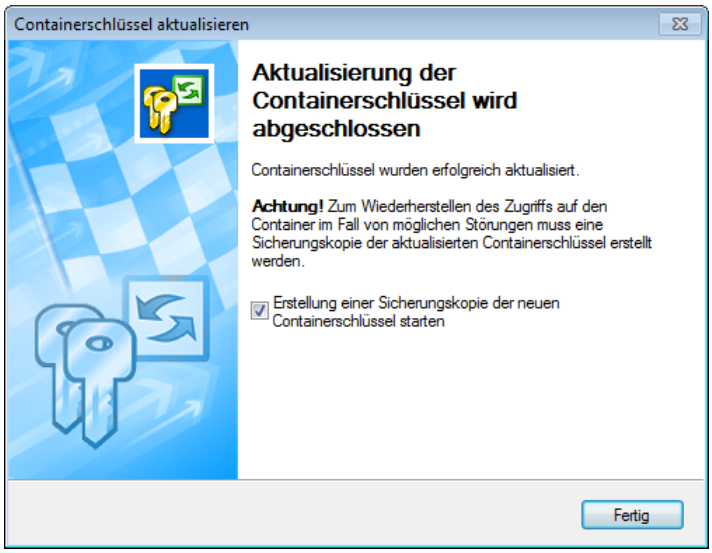
Containerschlüssel aktualisieren
Aktualisierung der Containerschlüssel wird abgeschlossen
Containerschlüssel wurden erfolgreich aktualisiert.
Achtung! Zum Wiederherstellen des Zugriffs auf den Container im Fall von möglichen Störungen muss eine Sicherungskopie der aktualisierten Containerschlüssel erstellt werden.
Erstellung einer Sicherungskopie der neuen Containerschlüssel starten
Fertig

Abbildung 50: Containerschlüssel-Aktualisierung abschließen

Auf dieser Seite ist das Kontrollkästchen **Erstellung einer Sicherungskopie der neuen Containerschlüssel starten** standardmäßig aktiviert. Die Sicherungskopie der neuen Schlüssel wird sofort nach Abschluss des Assistenten angelegt. Deaktivieren Sie dieses Kontrollkästchen, um die Sicherungskopie der neuen Containerschlüssel zu einem späteren Zeitpunkt zu erstellen.

Achtung! Die Sicherungskopie der Containerschlüssel wird für die Wiederherstellung des Containerzugangs im Falle einer Schlüsselbeschädigung verwendet. Deswegen wird es ausdrücklich empfohlen, Sicherungskopien der Containerschlüssel zu erstellen.

Wenn Sie mit Hilfe einer Sicherungskopie der Containerschlüssel anderen Benutzern den Zugang zum Container auf Ihrem Computer gewährt haben (s. Containerzugang für einen oder mehrere Benutzer auf demselben oder auf unterschiedlichen Computern bereitstellen auf Seite 123), können diese nach Abschluss der Schlüsselaktualisierung nicht mehr mit dem Container arbeiten. Wenn Sie den Containerzugang wieder bereitstellen wollen, überreichen Sie eine Sicherungskopie der neuen Containerschlüssel an die entsprechenden Benutzer.

---

5 Klicken Sie auf **Fertig**, um die Arbeit des Assistenten abzuschließen.

Container-Datei verschieben

Damit Sie mit den Containern von bequem arbeiten können, können die Containerdateien in einen anderen Ordner, auf einen externen Datenträger oder auf ein Remote-Laufwerk kopiert oder auf eine CD geschrieben werden.

Um eine Container-Datei in einen anderen Ordner, auf ein externes Gerät oder ein Netzlaufwerk zu verschieben:

1. Öffnen Sie das Fenster mit den Container-Eigenschaften.
2. Geben Sie im Fenster **Container-Eigenschaften** in der Registerkarte **Container** im Feld **Container-Datei** den neuen Pfad zur Container-Datei an.
3. Klicken Sie auf **OK**.

Die Datei wird entsprechend dem neuen Pfad verschoben.

Wenn Sie vorhaben, mit Containern zu arbeiten, die auf einer CD gespeichert sind, dann sollte der neue Pfad der Containerdatei nach Abschluss des Schreibvorgangs im Fenster der Containereigenschaften angegeben werden. Auf einen Container, der auf einer CD gespeichert ist, kann nur lesend zugegriffen werden. Deswegen sollte für die ordnungsgemäße Verwendung des Containers das Kontrollkästchen **Nur zum Lesen einbinden** aktiviert werden.

Achtung! ViPNet SafeDisk unterstützt die Arbeit mit Container-Dateien, die auf CD im ISO und ISO+Joilet-Format gespeichert werden.

Container löschen

Vergewissern Sie sich vor dem Löschen eines Containers, dass Sie die im Container enthaltenen Daten notfalls wiederherstellen können. Eine Wiederherstellung der Daten ist möglich, falls zumindest eine der nachfolgenden Bedingungen erfüllt ist:

- Eine Exportdatei des Containers wurde erstellt (`*.sdx`).
- Eine Sicherungskopie der Containerschlüssel wurde erstellt (`*.sde`), welche zusammen mit einer Kopie der Container-Datei (`*.sdc`) an einem sicheren Ort aufbewahrt wird.

Achtung! Wenn Sie die oben genannten Dateien nicht angelegt haben, können Sie die Daten aus dem gelöschten Container nicht wiederherstellen.

Zum Löschen des Containers:

1. Trennen Sie den Container, falls er eingebunden ist .
2. Markieren Sie den Container und führen einen der folgenden Schritte aus:
   - Klicken Sie mit der rechten Maustaste auf den Container und wählen im Kontextmenü den Eintrag **Löschen**.
   - Wählen Sie im Menü **Container** den Befehl **Löschen**.
   - Drücken Sie die Taste **Entf**.
3. Aktivieren Sie im Fenster **Container löschen** die Kontrollkästchen **Ich will diesen Container tatsächlich löschen** und **Es ist mir bewusst, dass die Informationen unwiderruflich gelöscht werden**.

Container löschen - CONTAINER1CAA
Achtung! Nach dem Löschen des Containers ist das Wiederherstellen der Informationen, die im Container gespeichert wurden, nicht mehr möglich.
Ich will diesen Container tatsächlich löschen
Es ist mir bewusst, dass die Informationen unwiderruflich gelöscht werden
Container löschen
Abbrechen

Abbildung 51: Warnung über das Löschen des Containers

4. Klicken Sie auf **Container löschen**.

Parameter von ViPNet SafeDisk einstellen

Zum Konfigurieren der Parameter von ViPNet SafeDisk:

1. Wählen Sie im Menü **SafeDisk** den Eintrag **Einstellungen**.
2. Öffnen Sie im Fenster **Einstellungen** die Registerkarte **Allgemein**.

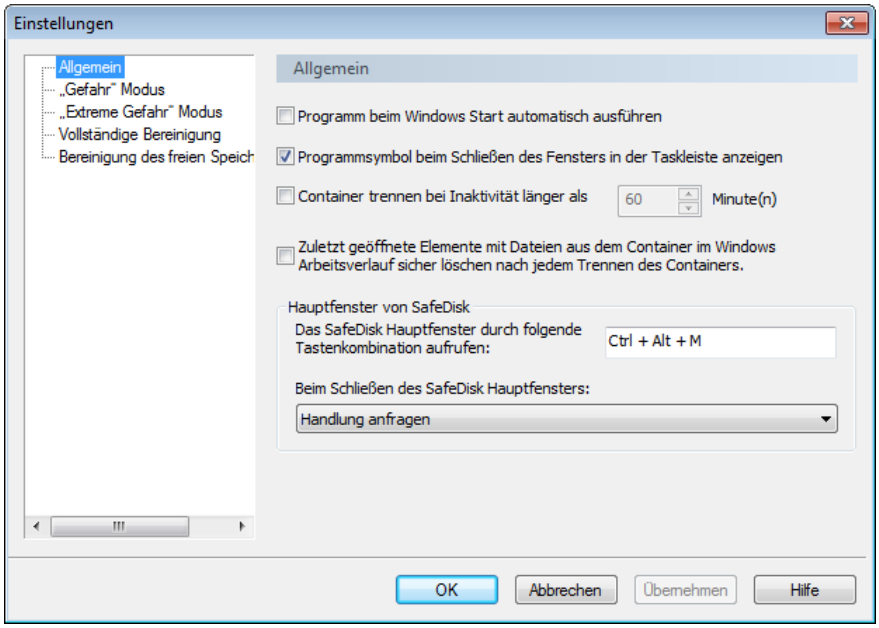

Abbildung 52: Einstellungen von ViPNet SafeDisk

3. Wenn Sie möchten, dass ViPNet SafeDisk automatisch beim Hochfahren von Windows gestartet wird, dann aktivieren Sie das Kontrollkästchen **Programm beim Windows Start automatisch ausführen**.
4. Wenn Sie nicht wollen, dass das Symbol von ViPNet SafeDisk im Infobereich der Taskleiste eingeblendet wird, dann deaktivieren Sie das Kontrollkästchen **Programmsymbol beim Schließen des Fensters in der Taskleiste anzeigen**.
5. Zum Einstellen der Leerlaufzeit, nach deren Ablauf die Container automatisch getrennt werden sollen, aktivieren Sie das Kontrollkästchen **Container trennen bei Inaktivität länger als** und geben die Zeit in Minuten an (standardmäßig ist der Wert 60 eingestellt).

6 Zum Bereinigen des Arbeitsverlaufs von zuletzt geöffneten Dokumenten nach Abschluss der Arbeit aktivieren Sie das Kontrollkästchen **Zuletzt geöffnete Elemente mit Dateien aus dem Container im Windows Arbeitsverlauf sicher löschen**.

7 Um den Hotkey-Tastaturbefehl zum Aufrufen des ViPNet SafeDisk Programmfensters zu ändern, klicken Sie in das Eingabefeld **Das SafeDisk Hauptfenster durch folgende Tastenkombination aufrufen** und drücken Sie eine neue Tastenkombination.

8 Zum Ändern der Aktion, die beim Anklicken der Schaltfläche **Schließen** ausgeführt wird, wählen Sie in der Liste **Beim Schließen des SafeDisk Hauptfensters** eine der folgenden Optionen aus: **Handlung anfragen**, **Das SafeDisk-Fenster verstecken ohne dabei das Programm zu schließen** oder **SafeDisk schließen**.

9 Wenn Sie die vorgenommenen Änderungen beibehalten wollen, klicken Sie auf **Übernehmen** und anschließend auf **OK**. Wenn Sie die Änderungen nicht speichern wollen, klicken Sie auf **Abbrechen**.

6

Geschützte Daten exportieren und importieren

Zweck des Exports und Imports geschützter Daten	95
Container exportieren	97
Container auf den Rechner importieren	100

Zweck des Exports und Imports geschützter Daten

Es kann manchmal erforderlich sein, mit geschützten Daten auch außerhalb des Büros zu arbeiten. Sie könnten zum Beispiel einen Bericht mit nach Hause nehmen, um ihn dort fertigzustellen. Dazu muss der Container mit privaten Daten zunächst von Ihrem Büro-Rechner auf Ihr privates Notebook übertragen werden. Das kann durch einen Export des ViPNet SafeDisk-Containers bewerkstelligt werden. Die Exportfunktionalität kann sowohl in der beschriebenen Situation als auch für die Erstellung von Sicherungskopien des Containers verwendet werden.

Nehmen wir an, dass Sie den Container auf Ihr Notebook exportiert und den Bericht beendet haben. Nun wollen Sie den Bericht an Ihren Vorgesetzten senden oder in ein Versionskontrollsystem hochladen. Nehmen wir zusätzlich an, dass Sie dies nur von Ihrem Büro-Rechner aus tun können (zum Beispiel aus Sicherheitsgründen). Um diese Aufgabe zu lösen, müssen Sie den fertigen Bericht zunächst von Ihrem Notebook auf den Büro-Computer übertragen. Ihr Bericht enthält sensible Daten, deswegen wollen Sie ihn nicht unter Verwendung konventioneller Methoden kopieren (mit Hilfe einer Diskette, eines USB-Sticks oder eines anderen mobilen Datenträgers). Der Bericht muss außerdem verschlüsselt bleiben. In diesem Fall können Sie das auf Ihrem Notebook installierte Programm ViPNet SafeDisk nutzen, um den Container mit dem Bericht zu exportieren. Anschließend können Sie mit Hilfe von ViPNet SafeDisk, das auf dem Büro-Rechner installiert ist, den Container importieren. Sie können die Importfunktionalität des Programms auch dazu verwenden, den Container aus einer Sicherungskopie wiederherzustellen.

Betrachten wir eine andere Situation. Sie fahren in den Urlaub, während Ihres Urlaubs müssen jedoch dringende Änderungen in ein von Ihnen erarbeitetes Projektkonzept eingebracht werden. Das Konzept enthält sensible Daten, deswegen kann es nicht ungeschützt übertragen werden. Sie können nun die Export- und Importmöglichkeiten von ViPNet SafeDisk nutzen, um dieses Problem zu lösen. Um das Dokument an eine Person zu übergeben, die während Ihrer Abwesenheit die notwendigen Änderungen vornehmen kann, können Sie den Container mit dem Bericht exportieren und ihn zusammen mit dem beim Export verwendeten Kennwort an diese Person weiterleiten. Ihr Vertreter kann den Container importieren, indem er das von Ihnen erhaltene Passwort benutzt. Nach Durchführung dieser Schritte kann Ihr Vertreter ungehindert mit den benötigten privaten Daten weiterarbeiten.

Nachfolgend sind Situationen aufgelistet, in denen die Import- und Exportfunktionalitäten von ViPNet SafeDisk von Nutzen sein könnten:

- Erstellung einer Sicherheitskopie oder Wiederherstellung privater Daten;

- Austausch geschützter Informationen zwischen zwei oder mehr Computern (sowohl über das Netzwerk als auch mit Hilfe mobiler Datenträger); auch wenn die Daten abgefangen werden, können sie dank der Verschlüsselung nicht angezeigt oder weiterverwendet werden;

- Sichere Übergabe geschützter Daten an weitere vertraute Personen.

- Update des Programms auf die Version 3.3.0. Im Zuge des Updates wird eine Konvertierung der Container durchgeführt. Es wird empfohlen, die Container vor der Konvertierung zu exportieren, um die Möglichkeit zu erhalten, mit diesen Containern in einer früheren Version von ViPNet SafeDisk wieder zu arbeiten.

Container exportieren

Beim Containerexport wird eine sogenannte Export-Datei des Containers erstellt. Sie sollten die Exportfunktionalität verwenden, wenn Sie folgende Aufgaben lösen wollen:

- Eine Sicherungskopie der im Container gespeicherten privaten Daten erstellen;
- vertrauliche Daten mit Hilfe eines Kuriers oder über das Netzwerk übertragen; private Daten während Ihrer Abwesenheit im Büro an einen Kollegen weiterleiten.

Zum Exportieren des Containers:

1. Wählen Sie im Programmfenster von ViPNet SafeDisk den Container aus, der exportiert werden soll. Wenn der Container eingebunden ist, trennen Sie ihn.
2. Wählen Sie im Menü **Container** den Befehl **Export**.
3. Geben Sie auf der ersten Seite des Assistenten **Container-Export** den Namen und den Pfad der Datei an, in welche der Container exportiert werden soll. Sie können die standardmäßig vorgegebenen Werte für Dateinamen und –pfad übernehmen oder auf die Schaltfläche klicken, um eine andere Datei auszuwählen. Klicken Sie anschließend auf **Weiter**.

Container-Export
Container-Export
Container-Export ermöglicht die Übertragung eines Containers in Form einer Export-Datei auf einen anderen Computer. Die Export-Datei kann auch als Sicherung eines Containers zur Vermeidung von Datenverlust verwendet werden.
Bestimmen Sie die Export-Datei für die Speicherung des Containers:
C:\Users\Fortress\Documents\CONTAINER1CAA.sdx
...
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 53: Assistent für den Container-Export

Tipp. Speichern Sie die Export-Datei des Containers aus Sicherheitsgründen nicht in demselben Ordner ab, in dem sich die Container-Datei befindet. Wir empfehlen, für die Speicherung der Container-Datei einen mobilen Datenträger zu verwenden.

4 Geben Sie auf der Seite **Passwort für die Export-Datei des Containers** ein Kennwort ein und wiederholen die Eingabe zur Bestätigung. Klicken Sie dann auf **Weiter**.

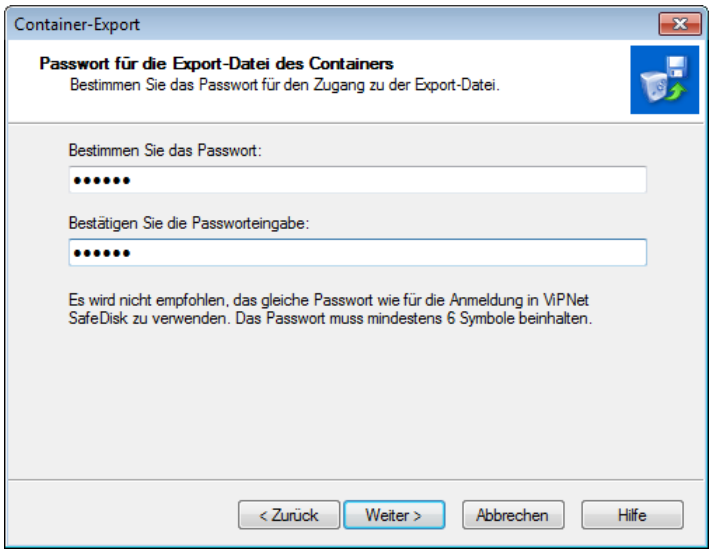
Container-Export
Passwort für die Export-Datei des Containers
Bestimmen Sie das Passwort für den Zugang zu der Export-Datei.
Bestimmen Sie das Passwort:
Bestätigen Sie die Passworteingabe:
Es wird nicht empfohlen, das gleiche Passwort wie für die Anmeldung in ViPNet SafeDisk zu verwenden. Das Passwort muss mindestens 6 Symbole beinhalten.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 54: Kennwort für die Export-Datei des Containers eingeben

5 Definieren Sie auf der Seite **Container-Eigenschaften** die Parameter des zu exportierenden Containers:

- Wenn Sie verhindern wollen, dass der Inhalt des exportierten Containers verändert werden kann, aktivieren Sie das Kontrollkästchen **Den Container nur zum Lesen verwenden**.
- Wenn Sie möchten, dass der exportierte Container nach dem Import automatisch eingebunden wird, aktivieren Sie das Kontrollkästchen **Den Container automatisch beim Start von ViPNet SafeDisk einbinden**.

Klicken Sie auf **Weiter**.

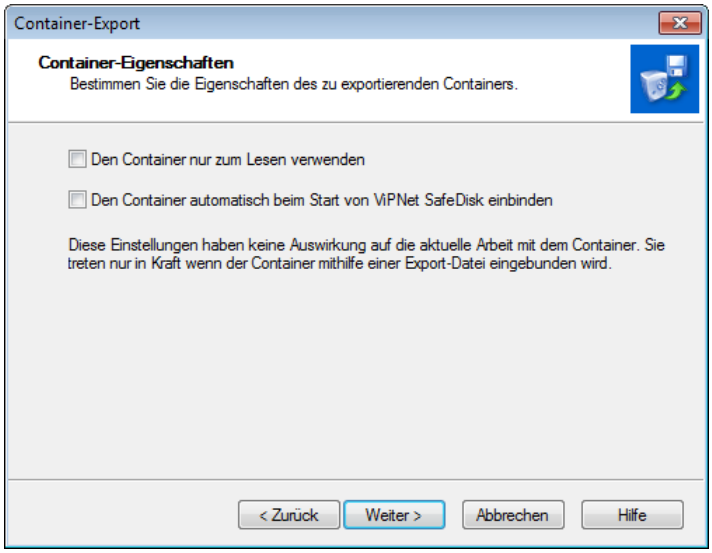
Container-Export
Container-Eigenschaften
Bestimmen Sie die Eigenschaften des zu exportierenden Containers.
Den Container nur zum Lesen verwenden
Den Container automatisch beim Start von ViPNet SafeDisk einbinden
Diese Einstellungen haben keine Auswirkung auf die aktuelle Arbeit mit dem Container. Sie treten nur in Kraft wenn der Container mithilfe einer Export-Datei eingebunden wird.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 55: Container-Eigenschaften definieren

6 Klicken Sie auf der Seite **Abschluss des Container-Exports** auf die Schaltfläche **Fertig**.

Es wird die Export-Datei des Containers `*.sdx` angelegt (s. Exportdatei des Containers auf Seite 179). Die Export-Datei beinhaltet die Container-Datei und eine Sicherungskopie der Containerschlüssel.

Sie können die neu erstellte Export-Datei des Containers mit Hilfe eines mobilen Datenträgers (CD, USB-Stick u. s. w.) oder über das Netzwerk (HTTP, FTP u. s. w.) auf einen anderen Computer übertragen.

Container auf den Rechner importieren

Container aus einer Export-Datei importieren

Sie sollten den Container aus einer Export-Datei importieren, wenn Sie folgende Aufgaben lösen müssen:

- Geschützte Daten aus einer Sicherungskopie wiederherstellen (s. Wiederherstellen des Zugriffs auf die geschützten Daten auf Seite 108).
- Mit geschützten Daten eines Kollegen während seiner Abwesenheit weiterarbeiten.

Damit der Container aus einer Export-Datei importiert werden kann, müssen Sie über folgende Objekte verfügen:

- Export-Datei des Containers (`*.sdx`);
- Kennwort, das beim Export des Containers verwendet wurde.

Führen Sie die folgenden Schritte aus, um den Container aus einer Export-Datei zu importieren:

1. Wählen Sie im Menü **Container** den Punkt **Import**. Der Assistent **Container-Import** wird gestartet.
2. Wählen Sie auf der Seite **Container-Import** die Option Datei und klicken auf **Weiter**.

Container-Import
Container-Import
Der Import ermöglicht den Zugriff auf einen Container falls früher eine Export-Datei des Containers oder eine Sicherungskopie der Containerschlüssel erstellt wurden.
Geben Sie an, welches Objekt für den Import verwendet werden soll:
Datei
Externes Authentisierungsgerät
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 56: Assistent für den Container-Import

3 Klicken Sie auf der Seite **Zugangspasswort** auf die Schaltfläche und geben Sie den Pfad zur Export-Datei des Containers an. Wählen Sie in der Liste **Dateityp** den Eintrag **Container-Export (*.sdx)** aus, um die Dateisuche zu beschleunigen.

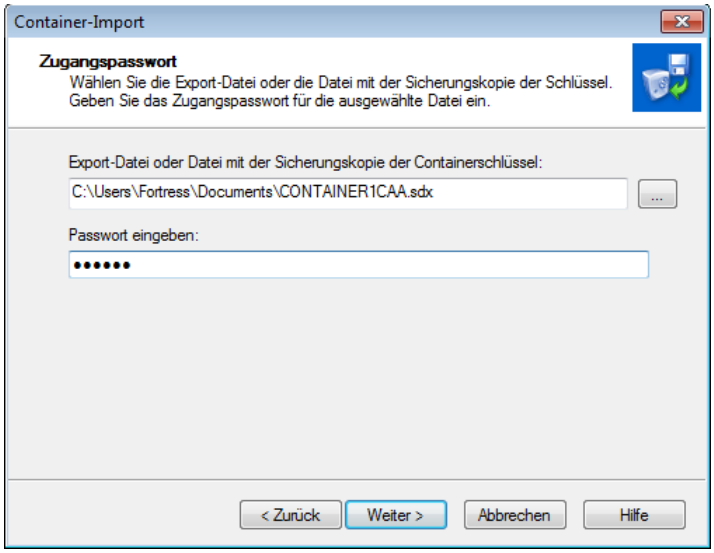

Abbildung 57: Zugangskennwort eingeben

4 Geben Sie im Feld **Passwort eingeben** das Kennwort ein, das beim Export des Containers verwendet wurde. Klicken Sie anschließend auf **Weiter**.

5 Geben Sie auf der Seite **Container-Datei** den Namen und den Pfad der Datei des Containers an, in welchem der zu importierende Container untergebracht werden soll.

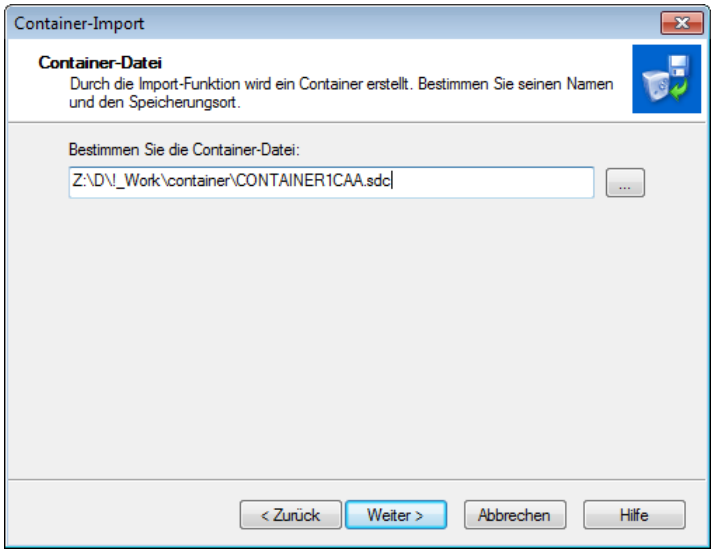

Abbildung 58: Speicherort des zu importierenden Containers bestimmen

6 Wenn die beim letzten Schritt definierte Container-Datei bereits existiert, geben Sie auf der Seite **Der Container existiert bereits** an, ob der bestehende Container vollständig ersetzt werden soll, oder ob nur die Schlüssel des bestehenden Containers ersetzt werden sollen.

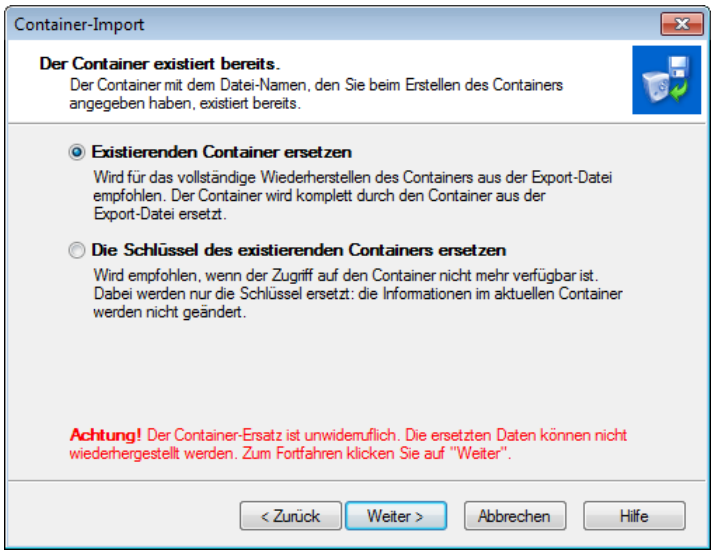
Container-Import
Der Container existiert bereits.
Der Container mit dem Datei-Namen, den Sie beim Erstellen des Containers angegeben haben, existiert bereits.
Existierenden Container ersetzen
Wird für das vollständige Wiederherstellen des Containers aus der Export-Datei empfohlen. Der Container wird komplett durch den Container aus der Export-Datei ersetzt.
Die Schlüssel des existierenden Containers ersetzen
Wird empfohlen, wenn der Zugriff auf den Container nicht mehr verfügbar ist. Dabei werden nur die Schlüssel ersetzt: die Informationen im aktuellen Container werden nicht geändert.
Achtung! Der Container-Ersatz ist unwiderruflich. Die ersetzten Daten können nicht wiederhergestellt werden. Zum Fortfahren klicken Sie auf "Weiter".
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 59: Bestimmen, ob der Container ersetzt wird

7 Wenn Sie nicht wollen, dass der Container sofort nach dem Import in einem separaten Fenster geöffnet wird, deaktivieren Sie im Fenster **Abschluss des Container-Imports** das Kontrollkästchen **Container einbinden**.

Klicken Sie auf **Fertig**.

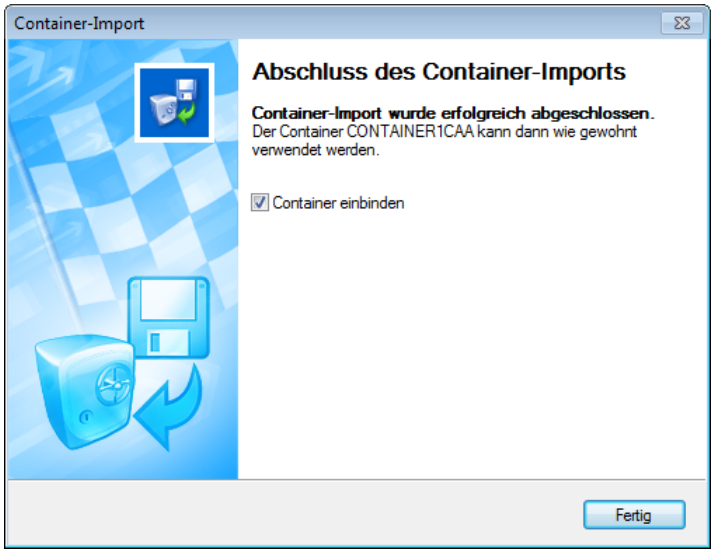

Abbildung 60: Abschluss des Container-Imports

Es wird ein neuer Container angelegt, der eine Kopie des importierten Containers darstellt. Der neue Container wird im Hauptfenster von ViPNet SafeDisk angezeigt.

Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren

In folgenden Fällen sollten Sie den Container mit Hilfe einer Sicherungskopie der Containerschlüssel importieren:

- Es wurden Schlüssel beschädigt, mit denen der Container verschlüsselt wurde. Wenn der Container selbst intakt ist, können Sie mit Hilfe der Sicherungskopie der Containerschlüssel den Zugang zu geschützten Daten wiederherstellen (s. Wiederherstellen des Zugriffs auf die geschützten Daten auf Seite 108).

- Für den Zugriff auf den Container haben Sie eine Schlüssel-Datei verwendet, welche nicht mehr vorhanden ist. Mit Hilfe der Sicherungskopie der Containerschlüssel werden Sie den Zugriff auf den Container wiederherstellen können.

- Sie arbeiten auf einem anderen PC und für Sie ist ein neues Benutzerkonto in ViPNet SafeDisk angelegt worden (s. Zugriff auf die geschützten Daten verwalten. Neuen Benutzer registrieren auf Seite 119).

- Sie erhalten die Container-Datei (jedoch nicht die Export-Datei des Containers) sowie eine Sicherungskopie der Schlüssel dieses Containers. Sie wollen den Container einbinden, um Zugriff auf die im Container gespeicherten privaten Daten zu erhalten.

Führen Sie die folgenden Schritte aus, um den Container mit Hilfe der Sicherungskopie seiner Schlüssel zu importieren:

1. Wählen Sie im Menü **Container** den Punkt **Import**. Es wird der Assistent **Container-Import** gestartet.

2. Gehen Sie auf der Seite **Container-Import** (s. Abbildung auf Seite 101) wie folgt vor:

   - Wenn die Sicherungskopie der Containerschlüssel in einer Datei auf dem Computer gespeichert ist, führen Sie die folgenden Schritte aus:

     - Wählen Sie die Option **Datei** und klicken Sie auf **Weiter**.
     - Klicken Sie auf der Seite **Zugangspasswort** (s. Abbildung auf Seite 101) auf die Schaltfläche und geben den Pfad zur Datei mit der Sicherungskopie der Containerschlüssel an. Wählen Sie in der Liste **Dateityp** den Eintrag **Sicherungskopie der Containerschlüssel (*.sde)** aus, um die Dateisuche zu beschleunigen.
     - Geben Sie im Feld **Passwort eingeben** das Kennwort ein, das beim Erstellen der Sicherungskopie der Containerschlüssel verwendet wurde. Klicken Sie anschließend auf **Weiter**.

   - Wenn die Sicherungskopie der Containerschlüssel auf einem externen Gerät gespeichert ist, führen Sie die folgenden Schritte aus:

     - Wählen Sie die Option **Externes Authentisierungsgerät** und klicken auf **Weiter**. Es wird die Seite **Externes Authentisierungsgerät auswählen** eingeblendet.

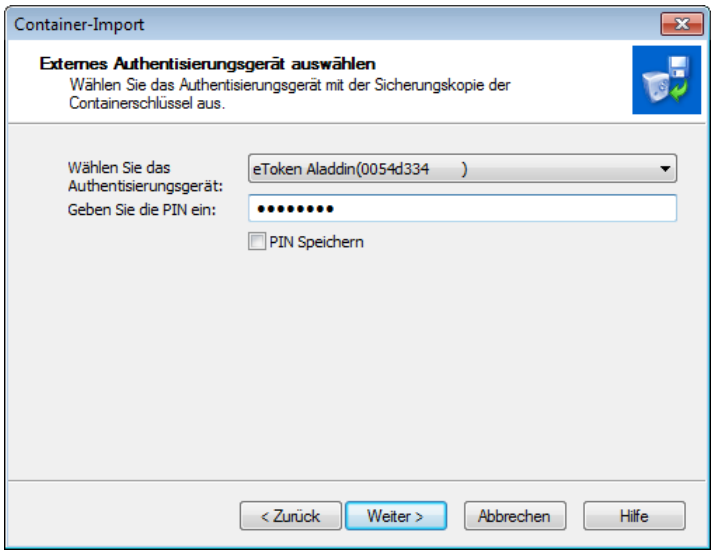

Abbildung 61: Externes Gerät auswählen

   - Stellen Sie sicher, dass das externe Gerät mit der entsprechenden Leseeinrichtung verbunden ist.

- Wählen Sie in der Liste **Wählen Sie das Authentisierungsgerät** das benötigte Gerät aus (wenn es nicht bereits automatisch ausgewählt wurde).

Hinweis. Die Sicherungskopie der Containerschlüssel (s. Sicherungskopie der Containerschlüssel erstellen auf Seite 70) muss vorher bereits auf dem ausgewählten Gerät gespeichert worden sein.

- Geben Sie im Feld **Geben Sie die PIN ein** den Zugangscode für das Gerät ein. Um die PIN zu speichern, aktivieren Sie das entsprechende Kontrollkästchen.
- Klicken Sie auf **Weiter**. Es wird die Seite **Sicherungskopie der Containerschlüssel auswählen** eingeblendet.

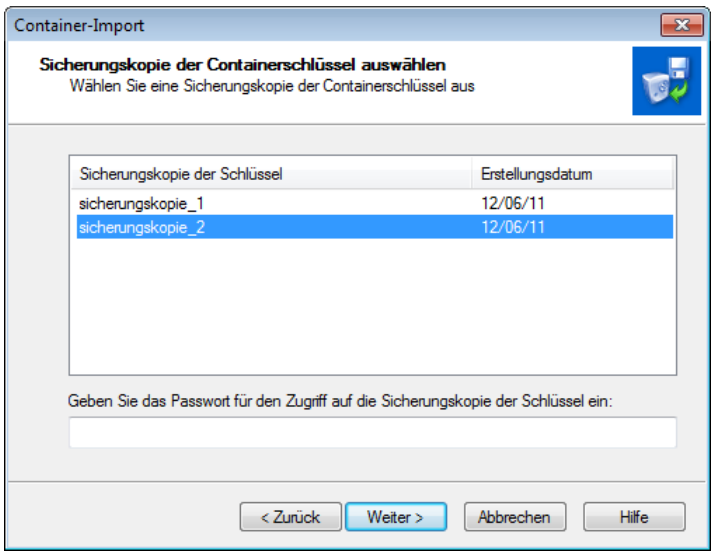

Abbildung 62: Sicherungskopie auswählen

- Wählen Sie aus der Liste der Sicherungskopien diejenige aus, die Sie für den Container-Import verwenden möchten.
- Geben Sie das Zugangspasswort für die gewählte Sicherungskopie der Schlüssel ein und klicken auf **Weiter**.

3 Wenn sich die Sicherungskopie der Containerschlüssel und die Container-Datei in unterschiedlichen Ordnern befinden, klicken Sie auf der Seite **Container-Datei** auf die Schaltfläche ... und geben Sie den Pfad zur Container-Datei an.

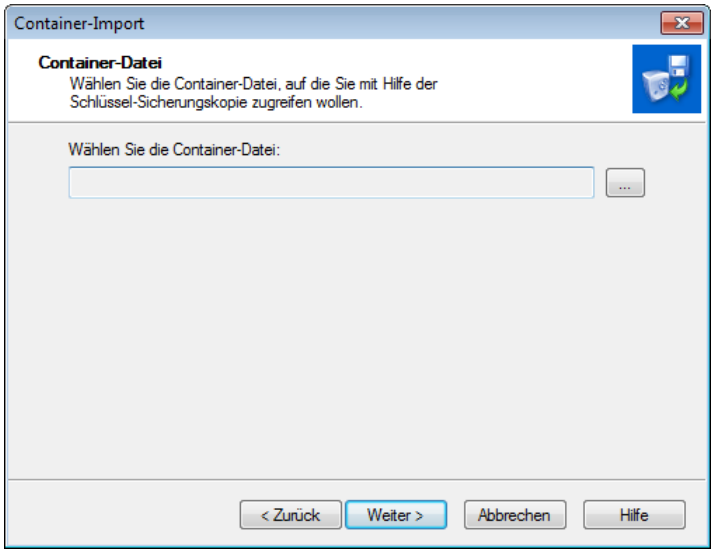

Abbildung 63: Pfad zur Container-Datei definieren

4 Auf der Seite **Zugriffstyp auf den Container** (s. Abbildung auf Seite 86) wählen Sie einen der möglichen Zugriffstypen: **Passwort**, **Schlüssel-Datei** oder **Authentisierungsgerät**.

Wenn Sie **Schlüssel-Datei** oder **Authentisierungsgerät** gewählt haben, führen Sie die entsprechenden Konfigurationsschritte durch (s. Container erstellen auf Seite 61).

5 Wenn Sie nicht wollen, dass der Container sofort nach dem Import in einem separaten Fenster geöffnet wird, deaktivieren Sie auf der Seite **Abschluss des Container-Imports (s. Abbildung auf Seite 103) das Kontrollkästchen Container einbinden.**

Klicken Sie auf **Fertig**.

Nach Abschluss des Assistenten sieht die Situation folgendermaßen aus:

- wenn Sie den Zugang zu einem Container wiederherstellen wollten, dessen Schlüssel beschädigt waren, wird der Zugang nun wieder hergestellt;
- wenn Sie die Sicherungskopie der Schlüssel verwendet haben, um eine Container-Datei zu importieren, wird der Container nun importiert, und Sie können beginnen, mit den im Container enthaltenen privaten Daten zu arbeiten.

Hinweis. Wenn Sie den Container aus einer Export-Datei importieren, dann wird ein neuer Container angelegt, der eine Kopie des importierten Containers darstellt.

Wenn Sie den Container mit Hilfe einer Sicherungskopie der Containerschlüssel importieren, dann erhalten Sie unmittelbar den Zugang zum importierten Container (eine Kopie wird nicht angelegt).

Sicherungskopie der Containerschlüssel auswählen

Die Seite **Sicherungskopie der Containerschlüssel auswählen** wird beim Import des Containers von einem externen Gerät angezeigt, falls die Verbindungsparameter zum externen Gerät korrekt angegeben wurden.

Auf dieser Seite werden Informationen über die Sicherungskopien der Schlüssel (Dateien mit der Erweiterung `*.sde`), die auf dem Gerät festgestellt wurden, aufgelistet: es werden der Name und das Erstellungsdatum angezeigt.

Zum Fortsetzen der Arbeit wählen Sie in der Liste die Sicherungskopie der Schlüssel desjenigen Containers aus, der importiert werden soll, und geben Sie anschließend im Feld **Geben Sie das Passwort für den Zugriff auf die Sicherungskopie der Schlüssel ein** das Passwort ein. Klicken Sie dann auf **Weiter**.

7

Wiederherstellen des Zugriffs auf die geschützten Daten

Warum Daten wiederhergestellt werden müssen 109

Lösungsvorschläge für die Wiederherstellung geschützter Daten 110

Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen 112

Warum Daten wiederhergestellt werden müssen

Daten sind oft unbezahlbar. Wenn wichtige Informationen verloren gehen oder in die Hände von Übeltätern gelangen, kann das sowohl zu kleinen Unannehmlichkeiten als auch zu riesigen finanziellen Verlusten führen. Seit Computer aus dem täglichen Geschäftsleben nicht mehr wegzudenken sind, haben alle Organisationen das Bestreben, ihre Daten auf bestmöglichen Weg zu schützen.

Die regelmäßige Erstellung von Sicherungskopien ist eine der am weitesten verbreiteten Methoden, mit deren Hilfe Daten geschützt und im Notfall schnell wiederhergestellt werden können. Wenn mit der aktuellen Version Ihrer Daten etwas geschehen sollte, können Sie die Daten aus der letzten Sicherungskopie wiederherstellen. Auch wenn einige unwesentliche Änderungen verlorengehen, wird der grundlegende Teil der Daten erfolgreich wiederhergestellt, und Sie können schnell zum Normalbetrieb zurückkehren.

Sie können ViPNet SafeDisk für den Schutz Ihrer Daten verwenden, indem Sie regelmäßig Sicherungskopien aller Container, einiger ausgewählter Container oder nur der Containerschlüssel erstellen.

Lösungsvorschläge für die Wiederherstellung geschützter Daten

Damit ein höheres Sicherheitsniveau gewährleistet werden kann, bietet ViPNet SafeDisk mehrere Methoden zur Wiederherstellung vertraulicher Daten an. Sie helfen dabei, bei Auftreten etwaiger Störungen die Arbeit mit den geschützten Daten schnell wieder fortzusetzen.

In der nachfolgenden Tabelle sind einige Problemfälle aufgelistet, die im Zuge der Verwendung privater Daten auftreten können. Daneben sind Empfehlungen für eine effektive Lösung der Probleme angegeben.

Tabelle 4. Empfehlungen für die Wiederherstellung geschützter Daten

Problem	Lösung
Zugriff auf alle Container nicht möglich	Es ist notwendig, die Wiederherstellung der Konfiguration durchzuführen. Für die Wiederherstellung wird die früher erstellte Sicherungskopie der Konfiguration benötigt, die Containerdateien dürfen dabei nicht beschädigt sein. Mehr dazu siehe unter Zugriff auf alle Container mittels der Konfigurationswiederherstellung ermöglichen (s. Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen auf Seite 112).
Zugriff auf einen oder mehrere Container nicht möglich	Es ist notwendig, den Zugriff auf den Container mit Hilfe der Sicherungskopie der Containerschlüssel wiederherzustellen. Dabei darf die Containerdatei nicht beschädigt sein. Mehr dazu siehe unter Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren (auf Seite 103).
Zugriffstyp auf den Container ändern	Den Zugriffstyp auf den Container können Sie auf der Registerkarte **Zugriffstyp** im Fenster **Eigenschaften** des Containers ändern. Außerdem können Sie den Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren und dabei den Zugriffstyp auf den Container ändern (s. Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren auf Seite 103).
Containerdatei ist beschädigt	Es ist notwendig, den Container zu importieren. Dafür wird die früher erstellte Export-Datei des Containers benötigt.
Hardwarefehler. Nur die Sicherungskopien	Die geschützten Daten können nicht wiederhergestellt werden wenn die Containerdatei beschädigt ist und wenn keine

der Containerschlüssel sind erhalten geblieben	Exportdatei des Containers vorhanden ist. Versuchen Sie, die Dateien auf der Festplatte wiederherzustellen. Nach der erfolgreichen Wiederherstellung kann der Container mit Hilfe der Sicherungskopie der Containerschlüssel wiederhergestellt werden. Es ist empfehlenswert, die Sicherungskopien der Container-Dateien regelmäßig anzulegen, um derartige Probleme zu vermeiden (s. Container exportieren auf Seite 97).
Hardwarefehler. Nur die Container-Datei ist erhalten geblieben	Wenn die Containerdatei vorhanden ist und die Containerschüssel verloren sind, können die geschützten Daten nicht wiederherstellt werden. Versuchen Sie, die Containerschlüssel auf der Festplatte wiederherzustellen. Nach der erfolgreichen Wiederherstellung können Sie diesen Container importieren. Es ist empfehlenswert, die Sicherungskopien der Container-Schlüssel regelmäßig anzulegen, um derartige Probleme zu vermeiden (s. Container exportieren auf Seite 97).

Achtung! Damit der Arbeitsablauf bei der Erstellung von Sicherungskopien und bei der Wiederherstellung von Daten vereinfacht werden kann, empfehlen wir, regelmäßig folgende Aktionen durchzuführen:

- Export-Dateien des Containers erstellen;
- Sicherungskopien der Containerschlüssel erstellen;
- Sicherungskopien der Konfiguration erstellen.

Wenn Sie sich an diese Empfehlungen halten, werden Sie Ihre vertraulichen Daten im Fall von unvorhersehbaren Störungen leicht wiederherstellen und den Zeitaufwand für die Wiederherstellung von Änderungen, die nach der letzten Sicherung vorgenommen wurden, deutlich reduzieren können.

Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen

Wenn der Zugang zu keinem Ihrer Containern mehr möglich ist, besteht der beste Weg zum Wiederherstellen der Daten in einer **Wiederherstellung der Konfiguration**.

Damit eine bestimmte Konfiguration wiederhergestellt werden kann, muss eine Sicherungskopie dieser Konfiguration rechtzeitig angelegt werden. Sie können so viele Sicherungskopien erstellen wie nötig sind.

Die Sicherungskopien der ViPNet SafeDisk-Konfiguration werden außerdem automatisch erstellt, wenn Sie sich im Programm abmelden oder eine Konfiguration wiederherstellen.

Sicherungskopie der Konfiguration erstellen

Eine Sicherungskopie der Konfiguration wird erstellt, um nachträglich die aktuelle Konfiguration des Programms wieder herstellen zu können.

Achtung! Wenn mehrere Benutzer mit einer Instanz von ViPNet SafeDisk arbeiten, muss jeder von ihnen seine eigenen Sicherungskopien der Konfiguration anlegen. Jeder Benutzer kann nur auf die von ihm selbst erstellten Sicherungskopien zugreifen.

Zum Erstellen einer Sicherungskopie der Konfiguration:

1. Trennen Sie alle eigebundenen Container.
2. Wählen Sie im Menü **SafeDisk** den Befehl **Wiederherstellung der Konfiguration**. Es wird der Assistent **Wiederherstellen der ViPNet SafeDisk Konfiguration** gestartet.
3. Aktivieren Sie auf der Seite **Wiederherstellung der ViPNet SafeDisk Konfiguration** die Option **Sicherungskopie der aktuellen Konfiguration erstellen** und klicken auf **Weiter**.

Wiederherstellen der ViPNet SafeDisk Konfiguration
Wiederherstellung der ViPNet SafeDisk Konfiguration
Die Wiederherstellung der Konfiguration ermöglicht es, zu einer früheren Version der ViPNet SafeDisk Konfiguration zurückzukehren. Für die Wiederherstellung werden die Sicherungskopien der Konfiguration verwendet, die automatisch in ViPNet SafeDisk erstellt werden. Sie können diese jederzeit auch manuell erstellen.
Wählen Sie die benötigte Option und klicken Sie auf Weiter.
ViPNet SafeDisk Konfiguration wiederherstellen
Sicherungskopie der aktuellen Konfiguration erstellen
Die Liste der Sicherungskopien ändern
Die letzte Wiederherstellung widerrufen
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 64: Assistent zum Wiederherstellen einer ViPNet SafeDisk-Konfiguration

4 Geben Sie auf der Seite **Erstellen der Sicherungskopie** im Eingabefeld **Kommentar zur Sicherungskopie** einen Kommentar mit der Beschreibung der Konfiguration ein. Die Eingabe eines Kommentars ist optional. Der Kommentar kann Ihnen jedoch später helfen, die benötigte Sicherungskopie schnell in der Übersicht zu finden. Die Länge des Kommentars ist auf 200 Zeichen beschränkt.

Klicken Sie auf **Weiter**. Es wird eine Sicherungskopie der aktuellen Konfiguration erstellt.

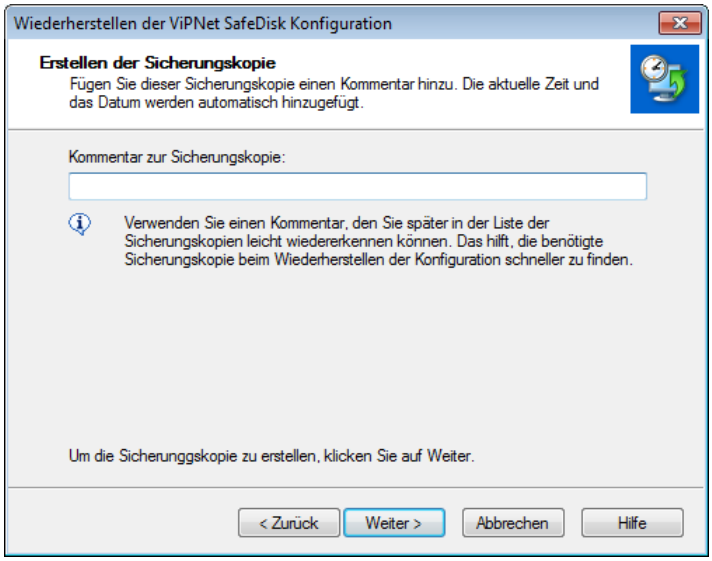
Wiederherstellen der ViPNet SafeDisk Konfiguration
Erstellen der Sicherungskopie
Fügen Sie dieser Sicherungskopie einen Kommentar hinzu. Die aktuelle Zeit und das Datum werden automatisch hinzugefügt.
Kommentar zur Sicherungskopie:
Verwenden Sie einen Kommentar, den Sie später in der Liste der Sicherungskopien leicht wiedererkennen können. Das hilft, die benötigte Sicherungskopie beim Wiederherstellen der Konfiguration schneller zu finden.
Um die Sicherunggskopie zu erstellen, klicken Sie auf Weiter.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 65: Sicherungskopie der Konfiguration erstellen

5 Klicken Sie auf der Seite **Abschluss der Erstellung der Sicherungskopie** auf **Fertig**, um den Assistenten abzuschließen.

Klicken Sie auf die Schaltfläche **Zum Anfang**, um eine neue Aktion mit Sicherungskopien durchzuführen.

Liste von Sicherungskopien der Konfiguration editieren

Sie können Ihre Liste der Sicherungskopien der Konfiguration editieren: Sicherungskopien löschen oder Kommentare bearbeiten.

Zum Editieren der Liste von Sicherungskopien der Konfiguration:

1. Trennen Sie alle Container.
2. Wählen Sie im Menü **SafeDisk** den Befehl **Wiederherstellung** der Konfiguration. Es wird der Assistent **Wiederherstellen der ViPNet SafeDisk Konfiguration** gestartet.
3. Aktivieren Sie auf der Seite **Wiederherstellung der ViPNet SafeDisk Konfiguration** die Option **Die Liste der Sicherungskopien ändern** und klicken anschließend auf **Weiter**.
4. Wählen Sie auf der Seite **Ändern der Liste der Sicherungskopien** die Sicherungskopie aus, die Sie bearbeiten wollen. Wenn Sie den Kommentar zur Sicherungskopie ändern möchten, klicken Sie auf die Schaltfläche **Kommentar ändern**. Wenn Sie die Sicherungskopie löschen möchten, klicken Sie auf **Löschen**.

   Die Sicherungskopien der Konfiguration werden automatisch nach Erstellungsdatum und -zeit sortiert. Zum Ändern der Sortierreihenfolge klicken Sie auf die Spaltenüberschrift **Erstellungszeit und -Datum** oder auf **Kommentar**.

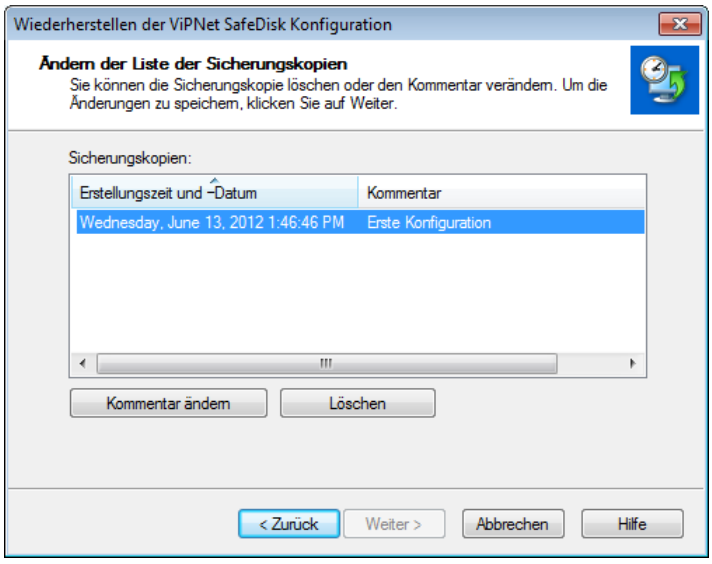

Abbildung 66: Ändern der Liste der Sicherungskopien

5. Klicken Sie auf **Weiter**, um die Bearbeitung abzuschließen.

6 Klicken Sie auf der Seite **Bearbeitung der Liste der Sicherungskopien abschließen** auf **Fertig**, um den Assistenten abzuschließen.

Klicken Sie auf die Schaltfläche **Zum Anfang**, um eine weitere Aktion mit Sicherungskopien durchzuführen.

Konfiguration wiederherstellen

Um die Konfiguration von ViPNet SafeDisk aus einer Sicherungskopie wiederherzustellen, führen Sie die folgenden Schritte durch:

1 Trennen Sie alle Container.

2 Wählen Sie im Menü **SafeDisk** den Befehl **Wiederherstellung der Konfiguration**. Es wird der Assistent **Wiederherstellen der ViPNet SafeDisk Konfiguration** gestartet.

3 Aktivieren Sie auf der Seite **Wiederherstellung der ViPNet SafeDisk Konfiguration** die Option **ViPNet SafeDisk Konfiguration wiederherstellen** und klicken anschließend auf **Weiter**.

Wenn dieser Option nicht verfügbar ist, bedeutet das, dass keine Sicherungskopien der Konfiguration erstellt wurden. In diesem Fall kann der Zugang zu diesem Container mit Hilfe der Importfunktionalität unter Verwendung einer Sicherungskopie seiner Schlüssel oder einer Export-Datei dieses Containers wiederhergestellt werden (s. Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren auf Seite 103).

4 Auf der Seite **Auswahl der Sicherungskopie** ist eine Liste aller Sicherungskopien der Konfiguration aufgeführt.

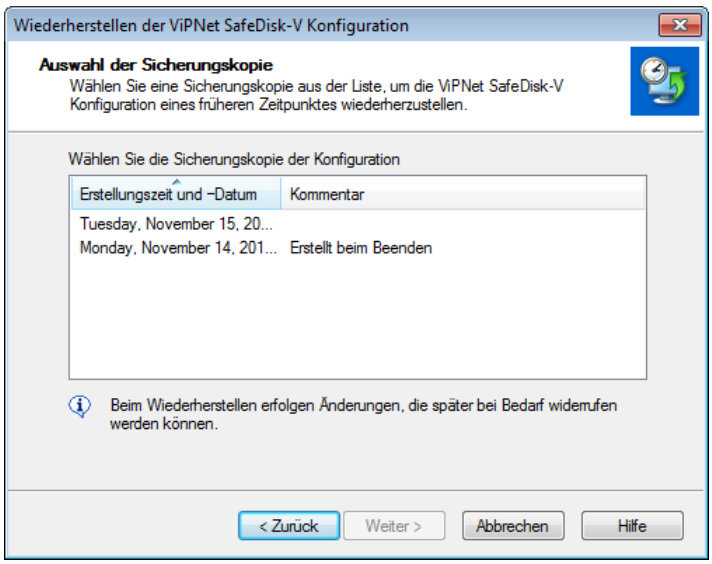
Wiederherstellen der ViPNet SafeDisk-V Konfiguration
Auswahl der Sicherungskopie
Wählen Sie eine Sicherungskopie aus der Liste, um die ViPNet SafeDisk-V Konfiguration eines früheren Zeitpunktes wiederherzustellen.
Wählen Sie die Sicherungskopie der Konfiguration
Erstellungszeit und -Datum
Kommentar
Tuesday, November 15, 20...
Monday, November 14, 201...
Erstellt beim Beenden
Beim Wiederherstellen erfolgen Änderungen, die später bei Bedarf widerrufen werden können.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 67: Sicherungskopie auswählen

Die Sicherungskopien der Konfiguration werden automatisch nach Erstellungsdatum und -zeit sortiert. Zum Ändern der Sortierreihenfolge klicken Sie auf die Spaltenüberschrift Erstellungszeit und -Datum oder auf Kommentar.

Wählen Sie die Sicherungskopie der ViPNet SafeDisk-Konfiguration, die Sie wiederherstellen möchten, und klicken auf **Weiter**.

5 Wenn Ihr Benutzerpasswort in SafeDisk nachdem Sie die Sicherungskopie erstellt haben geändert wurde, geben Sie im Fenster **Passwort** das alte Passwort ein, welches zum Zeitpunkt der Erstellung benutzt wurde und klicken Sie auf **Weiter**.

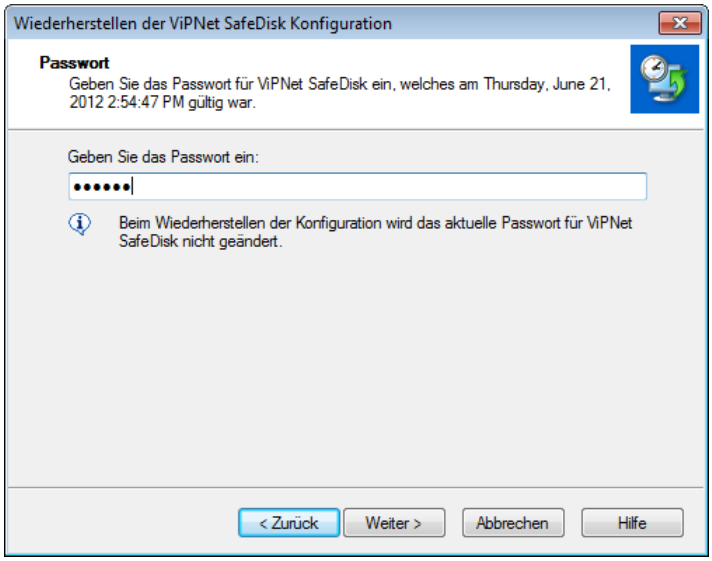
Wiederherstellen der ViPNet SafeDisk Konfiguration
Passwort
Geben Sie das Passwort für ViPNet SafeDisk ein, welches am Thursday, June 21, 2012 2:54:47 PM gültig war.
Geben Sie das Passwort ein:
Beim Wiederherstellen der Konfiguration wird das aktuelle Passwort für ViPNet SafeDisk nicht geändert.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 68: Eingabe des Passworts

6 Es wird der Vorgang zur Wiederherstellung der ausgewählten Konfiguration von ViPNet SafeDisk gestartet.

7 Klicken Sie auf der Seite **Abschluss der Wiederherstellung der ViPNet SafeDisk-Konfiguration** auf die Schaltfläche **Fertig**, um den Assistenten abzuschließen.

Klicken Sie auf die Schaltfläche **Zum Anfang**, um eine weitere Aktion mit Sicherungskopien durchzuführen.

Achtung! Wenn Sie nach der Wiederherstellung der Konfiguration immer noch kein Zugriff auf die Container haben, sind möglicherweise die Containerdateien beschädigt. In diesem Fall versuchen Sie jeden einzelnen Container aus der entsprechenden Export-Datei separat zu importieren. Dazu sollten Sie über bereits früher erstellte Export-Dateien der Container verfügen (s. Container exportieren auf Seite 97).

Letzte Wiederherstellung der Konfiguration rückgängig machen

Wenn die Wiederherstellung der Konfiguration das Problem nicht gelöst hat, können Sie zu einer früheren Konfiguration zurückkehren. Dazu müssen Sie die zuletzt durchgeführte Wiederherstellung der Konfiguration widerrufen.

Damit die letzte Wiederherstellung der Konfiguration rückgängig gemacht wird:

1. Trennen Sie alle Container.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie im Menü **SafeDisk** den Befehl **Wiederherstellung der Konfiguration**.
   - Klicken Sie auf der letzten Seite des Assistenten **Wiederherstellen der ViPNet SafeDisk Konfiguration** auf die Schaltfläche **Zum Anfang**.
3. Aktivieren Sie auf der Seite **Wiederherstellung der ViPNet SafeDisk Konfiguration** die Option **Die letzte Wiederherstellung widerrufen** und klicken anschließend auf **Weiter**.

Wiederherstellen der ViPNet SafeDisk Konfiguration
Wiederherstellung der ViPNet SafeDisk Konfiguration
Die Wiederherstellung der Konfiguration ermöglicht es, zu einer früheren Version der ViPNet SafeDisk Konfiguration zurückzukehren. Für die Wiederherstellung werden die Sicherungskopien der Konfiguration verwendet, die automatisch in ViPNet SafeDisk erstellt werden. Sie können diese jederzeit auch manuell erstellen.
Wählen Sie die benötigte Option und klicken Sie auf Weiter.
ViPNet SafeDisk Konfiguration wiederherstellen
Sicherungskopie der aktuellen Konfiguration erstellen
Die Liste der Sicherungskopien ändern
Die letzte Wiederherstellung widerrufen
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 69: Die letzte Wiederherstellung der Konfiguration wiederrufen

4. Klicken Sie auf der Seite **Widerruf der letzten Konfigurationswiederherstellung abschließen** auf die Schaltfläche **Fertig**, um den Assistenten abzuschließen.

   Klicken Sie auf die Schaltfläche **Zum Anfang**, um eine weitere Aktion mit Sicherungskopien durchzuführen.

8

Gemeinsame Nutzung von ViPNet SafeDisk

Zugriff auf die geschützten Daten verwalten. Neuen Benutzer registrieren 119

Zugriff auf die Container für mehrere Benutzer einrichten 121

Auf dem Server gespeicherte Daten schützen 130

Vertrauliche Daten mit Hilfe eines Kuriers oder über das Netzwerk übertragen 132

Zugriff auf die geschützten Daten verwalten. Neuen Benutzer registrieren

In ViPNet SafeDisk können mehrere Benutzer unabhängig von einander arbeiten, jeder Benutzer hat Zugriff nur auf seine geschützten Daten.

In folgenden Fällen ist es empfehlenswert, mehrere Benutzer in ViPNet SafeDisk anzulegen:

- Ein Notebook wird von verschiedenen Mitarbeitern für ihre Dienstreisen verwendet. In ViPNet SafeDisk kann jeder Mitarbeiter seine sensiblen Daten sicher speichern, ohne dabei den Zugriff auf die anderen Daten zu bekommen.
- Wenn auf dem PC mehrere Benutzerprofile angelegt sind und mehrere Benutzer mit ViPNet SafeDisk ihre sensiblen Daten schützen wollen.
- Wenn ViPNet SafeDisk nur auf einem PC installiert ist und Sie für die Zeit Ihres Urlaubs oder aus anderen Gründen den Zugriff auf einen Teil Ihrer sensiblen Daten einer vertrauten Person erlauben wollen, wollen aber gleichzeitig vermeiden, dass alle Ihre Daten angesehen oder verändert werden können, können Sie unter Windows und in ViPNet SafeDisk einen neuen Benutzer anlegen und die Sicherungskopie der Schlüssel für die Container, welche für die gemeinsame Nutzung bestimmt sind, der vertrauten Person zur Verfügung stellen.
- Sie wollen einen fiktiven Benutzer anlegen. Unter seinem Benutzerkonto erstellen Sie fiktive Container, die Sie mit unechten Daten befüllen. Sobald Sie über das Näherkommen Unbefugter erfahren, melden Sie sich in ViPNet SafeDisk mit dem fiktiven Benutzernamen an.

Jeder Benutzer hat Zugriff nur auf seine eigenen, von ihm erstellten Container.

Um einen neuen Benutzer anzulegen, führen Sie die folgenden Schritte durch:

1 Starten Sie ViPNet SafeDisk (s. ViPNet SafeDisk starten auf Seite 29).

Hinweis. Wenn das Programm ViPNet SafeDisk bereits gestartet ist, verlassen Sie das Programm, um die Arbeit unter diesem Benutzerprofil zu beenden (s. ViPNet SafeDisk starten auf Seite 29).

2 Im Passworteingabefenster klicken Sie auf **das Passwort für den neuen Benutzer erstellen**.

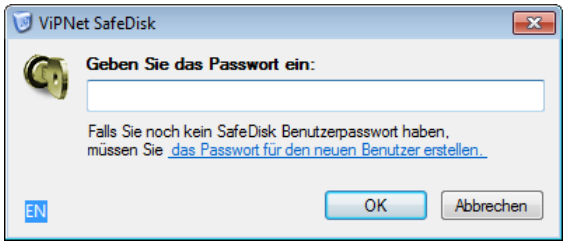

Abbildung 70: Passworteingabefenster

Das Fenster **Benutzerpasswort SafeDisk** öffnet sich.

3 Im Fenster **Benutzerpasswort SafeDisk** aus der Dropdown-Liste **Passworttyp** wählen Sie **Benutzerdefiniert** oder **Zufällig**. Mehr dazu lesen Sie im Abschnitt Benutzerpasswort definieren (auf Seite 37).

Zugriff auf die Container für mehrere Benutzer einrichten

Mit Hilfe von ViPNet SafeDisk können Sie den Zugang zu Ihren Containern auch anderen Benutzern zur Verfügung stellen, um gemeinsam mit geschützten Daten, die in diesen Containern gespeichert sind, arbeiten zu können.

Der allgemeine Zugang zu Containern kann auf zwei Arten eingerichtet werden:

1. Den Zugang zu Ihrem Container einem oder mehreren Benutzern auf demselben Computer oder auf unterschiedlichen Computern zur Verfügung stellen (s. Containerzugang für einen oder mehrere Benutzer auf demselben oder auf unterschiedlichen Computern bereitstellen auf Seite 123). Dazu müssen Sie entweder eine Sicherungskopie der Containerschlüssel an die Benutzer weiterleiten (falls diese Benutzer den gleichen Rechner verwenden wie Sie), oder die Container-Datei selbst mitsamt einer Sicherungskopie der Schlüssel dieses Containern bereitstellen (wenn diese Benutzer andere Rechner verwenden). Bei dieser Art des allgemeinen Containerzugangs ist die gleichzeitige gemeinsame Arbeit an vertraulichen Daten, die im entsprechenden Container gespeichert sind, nicht möglich. Auch wenn sich der Container auf einem Netzlaufwerk befindet, können mehrere Benutzer nicht gleichzeitig mit dem Container arbeiten.
2. Den allgemeinen Zugang zu Ihren Containern über das Netzwerk einrichten (s. Netzwerkzugang auf einen Container für mehrere Benutzer ermöglichen auf Seite 124). Bei dieser Art des Containerzugangs gewähren Sie den Zugang nicht zur Container-Datei selbst, sondern zum Laufwerk, das dem eingebundenen Container unter Windows entspricht. Sie erhalten dadurch die volle Kontrolle darüber, wer und wann auf Ihre geschützten Daten zugreifen darf.

Der erste Ansatz eignet sich gut für Situationen, in welchen ein Kollege Ihre Arbeit fortsetzen soll, weil Sie zum Beispiel in Urlaub gehen. In diesem Fall muss zunächst eine Sicherungskopie der Containerschlüssel an diesen Kollegen weitergeleitet werden. Er muss sich in ViPNet SafeDisk mit seinem Kennwort anmelden und den Container mit Hilfe der Sicherungskopie der Schlüssel importieren. Wenn dieser Mitarbeiter keinen Zugang zu Ihrem Rechner hat, müssen Sie ihm die Container-Datei und eine Sicherungskopie der Schlüssel dieses Containers übergeben.

Der zweite Ansatz scheint passend, wenn die gemeinsame Arbeit an sensiblen Dokumenten im Vordergrund steht. Nehmen wir an, Sie erstellen ein Projektkonzept. Nun wollen Sie dieses Konzept mit den Teamkollegen besprechen und mögliche Verbesserungen in das entsprechende

Dokument eintragen lassen. Dazu muss der Container, der das Konzept enthält, zuerst eingebunden, und der Zugang zum Laufwerk, das diesem Container unter Windows zugeordnet ist, für andere Benutzer freigegeben werden.

Beim Einrichten einer Freigabe der Container unter Verwendung des zweiten Ansatz sollten Sie sich mit den Möglichkeiten und Einschränkungen beim Bereitstellen des öffentlichen Zugangs zu den Containern vertraut machen (s. Abgrenzung des Containerzugangs auf Seite 122).

Hinweis. Diese Einschränkungen betreffen nur der zweite Ansatz zur Einrichtung der Container-Freigabe.

Abgrenzung des Containerzugangs

Die Abgrenzung des Containerzugangs kann grundsätzlich in zwei Typen unterteilt werden:

- Zugangsbeschränkungen in Abhängigkeit vom Dateisystem, in dem der Container formatiert wurde;
- Zugangsbeschränkungen in Abhängigkeit vom verwendeten Betriebssystem.

Die einzelnen Abhängigkeiten bei den Zugangsbeschränkungen sind in der unteren Tabelle aufgeführt.

Tabelle 5. Abgrenzung des Containerzugangs

<table>
<tr><th rowspan="2">Verwendetes Betriebssystem</th><th colspan="2">Dateisystem des Containers</th></tr>
<tr><th>NTFS</th><th>FAT / FAT32</th></tr>
<tr><td>Microsoft Windows XP SP3 (32-Bit)/Server 2003 (32/64-Bit)</td><td colspan="2">Wenn beim Einbinden des Containers das Kontrollkästchen Exklusiver Zugriff aktiviert wurde, dann werden die Berechtigungen für das Laufwerk, das dem Container entspricht, so festgelegt, dass mit Ausnahme des Benutzers, der den Container eingebunden hat, niemand sonst irgendwelche Aktionen in Bezug auf dieses Laufwerk ausführen kann, unabhängig davon, welche Berechtigungen für dieses Laufwerk im Betriebssystem festgesetzt wurden. Ebenso wird es nicht möglich sein, einen Netzwerkzugang zu diesem Laufwerk einzurichten. Einerseits kann dadurch die Sicherheit der Arbeit in Situationen, wenn mehrere Benutzer gleichzeitig auf einem Computer arbeiten können, wesentlich erhöht werden. Andererseits werden dadurch die Möglichkeiten zur gemeinsamen Arbeit mehrerer Benutzer mit einem Container eingeschränkt.

Wenn beim Einbinden des Containers das Kontrollkästchen Exklusiver Zugriff nicht aktiviert wurde, dann werden Berechtigungen wirksam, die für die Betriebssysteme Vista SP2 (32/64-Bit)/Server 2008 (32/64-Bit)/Windows 7 (32/64-Bit) gelten und weiter unten beschrieben sind.</td></tr>
<tr><td>Vista SP2 (32/64-Bit)/Server 2008 (32/64-Bit)/Windows 7 (32/64-Bit)</td><td>Beim Einbinden des Containers werden die Berechtigungen so festgelegt, dass nur der Benutzer, der den Container im Programm ViPNet SafeDisk eingebunden hat, den vollen Zugriff auf das Laufwerk, das dem Container entspricht, besitzt.

Beim Bereitstellen des öffentlichen Zugangs zum Container über das Netzwerk kann der Zugang der Benutzer zum Laufwerk, das dem Container entspricht, mit Hilfe der Betriebssystem-Werkzeuge erlaubt oder blockiert werden.</td><td>Vollständiger Zugriff aller Benutzer auf die Container.</td></tr>
</table>

Containerzugang für einen oder mehrere Benutzer auf demselben oder auf unterschiedlichen Computern bereitstellen

Zum Einrichten des Containerzugangs für andere Benutzer:

1 Wenn eine Sicherungskopie der Containerschlüssel noch nicht angelegt wurde, erstellen Sie diese (s. Sicherungskopie der Containerschlüssel erstellen auf Seite 70).

2 Leiten Sie die Sicherungskopie der Containerschlüssel (Datei *.sde) und das Kennwort, das beim Anlegen der Sicherungskopie verwendet wurde, an den Benutzer weiter, dem Sie den Zugang zum Container gewähren möchten.

3 Wenn der Zugang für einen Benutzer eingerichtet werden soll, der auf einem anderen Computer arbeitet, übergeben Sie ihm auch die Container-Datei (*.sdc).

Achtung! Wenn Sie mit Hilfe einer Sicherungskopie der Schlüssel einem anderen Benutzer den Zugang zum Container auf Ihrem Rechner gewährt und später die Schlüssel dieses Containers aktualisiert haben (s. Containerschlüssel aktualisieren auf Seite 88), dann verliert der andere Benutzer die Zugangsmöglichkeit wieder. Um die Arbeit mit Ihrem Container fortsetzen zu können, muss dieser Benutzer den Container mit Hilfe einer Sicherungskopie der neuen Schlüssel nochmals importieren.

Wenn ein anderer Benutzer den Zugang zu seinem Container bereitstellt:

1 Starten Sie ViPNet SafeDisk.

2 Wählen Sie im Menü **Container** den Befehl **Import**. Es wird der Assistent **Container-Import** gestartet.

3 Führen Sie den Import des Containers mit Hilfe einer Sicherungskopie seiner Schlüssel durch.

Nach Abschluss des Importvorgangs verfügen beide Benutzer über den Zugang zum Container. Wenn Sie die Sicherungskopie der Containerschlüssel an mehrere Benutzer übergeben haben, sind diese Benutzer nun ebenfalls imstande, auf den Container zuzugreifen. Es kann aber jeweils nur ein Benutzer zur gleichen Zeit mit dem Container arbeiten.

Netzwerkzugang auf einen Container für mehrere Benutzer ermöglichen

Damit mehrere Benutzer gleichzeitig oder anwechselnd mit geschützten Daten in Ihrem Container arbeiten können, muss das Laufwerk, das den Container im Betriebssystem Windows repräsentiert, für diese Benutzer freigegeben werden. Dadurch können Sie auch Benutzern, die ViPNet SafeDisk nicht auf ihren Rechnern installiert haben, den Zugriff auf die Daten in Ihrem Container erlauben.

Achtung! Seien Sie vorsichtig, wenn Sie den Containerzugang über das Netzwerk bereitstellen. Es werden auch Benutzer auf geschützte Daten in diesem Container zugreifen können, die ViPNet SafeDisk nicht installiert haben.

Hinweis. Beim Einbinden des Containers werden in den Betriebssystemen Windows Vista und höher die Rechte für die Ausführung der Dateien, die im Container enthalten sind, nur demjenigen Benutzer zugeteilt, unter dessen Konto der Container eingebunden wurde. Einige Programme dürfen nur mit Administratorrechten gestartet werden. Wenn demnach der Benutzer, der den Container eingebunden hat, über keine Administratorrechte verfügt, werden diese Programme nicht gestartet werden können.

Beim Auftreten einer solchen Situation wird empfohlen, die auszuführenden Dateien als Administrator zu starten oder dem Benutzer, der den Container einbindet, Administratorrechte zu erteilen.

Damit mehrere Benutzer gleichzeitig mit Ihren geschützten Daten arbeiten können, gehen Sie wie folgt vor:

1. Wählen Sie im Hauptfenster von ViPNet SafeDisk den Container aus, der für den allgemeinen Zugang bereitgestellt werden soll.
2. Binden Sie den gewählten Container ein, falls er noch nicht eingebunden ist (s. Einen früher erstellen Container einbinden auf Seite 77).
3. Öffnen Sie den Ordner **Arbeitsplatz** (über das Menü **Start** oder durch Anklicken des entsprechenden Symbols auf dem **Desktop**), klicken Sie mit der rechten Maustaste auf das Laufwerk, das dem gewählten Container entspricht, und wählen Sie im Kontextmenü den Eintrag **Freigabe und Sicherheit**. Es wird das Fenster **Eigenschaften von Lokaler Datenträger** eingeblendet.

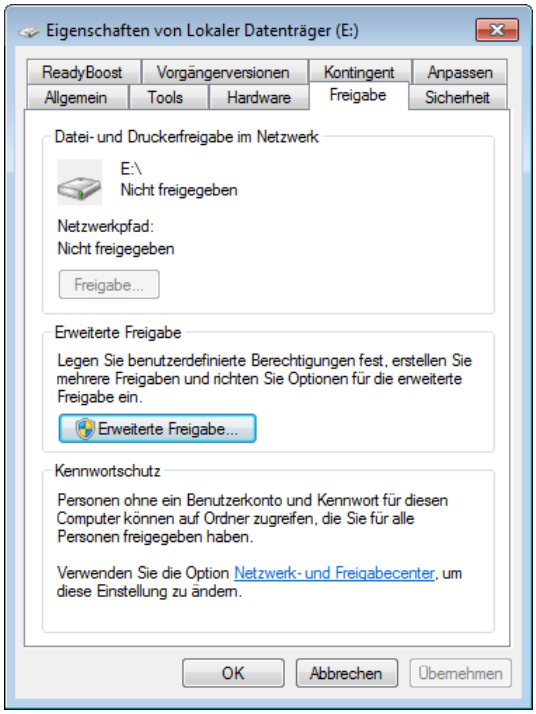

Abbildung 71: Fenster mit Eigenschaften des lokalen Laufwerks

4 In Windows Vista/Server 2008/Windows 7:

- Klicken Sie im Fenster **Eigenschaften von Lokaler Datenträger** in der Registerkarte **Freigabe** auf die Schaltfläche **Erweiterte Freigabe**.

- Aktivieren Sie im Fenster **Erweiterte Freigabe** das Kontrollkästchen **Diesen Ordner freigeben**. Geben Sie einen Namen für das freigegebene Objekt und die maximal zulässige Anzahl an Benutzern, die gleichzeitig darauf zugreifen können, an. Ebenso können Sie Zugriffsberechtigungen definieren (Schaltfläche **Berechtigungen**) und Einstellungen für den Offline-Modus konfigurieren (Schaltfläche **Zwischenspeichern**). Zusätzliche Informationen darüber finden Sie in der Windows-Hilfe.

Abbildung 72: Erweiterte Freigabe

In Windows XP/Server 2003:

- Aktivieren Sie im Fenster **Eigenschaften von Lokaler Datenträger** in der Registerkarte **Freigabe** die Option **Diesen Ordner freigeben**. Geben Sie einen Namen für das freigegebene Objekt und die maximal zulässige Anzahl an Benutzern, die gleichzeitig darauf zugreifen können, an. Zusätzlich können Sie Zugriffsberechtigungen definieren (Schaltfläche **Berechtigungen**) und Einstellungen für den Offline-Modus konfigurieren (Schaltfläche **Zwischenspeichern**). Zusätzliche Informationen darüber finden Sie in der Windows-Hilfe.

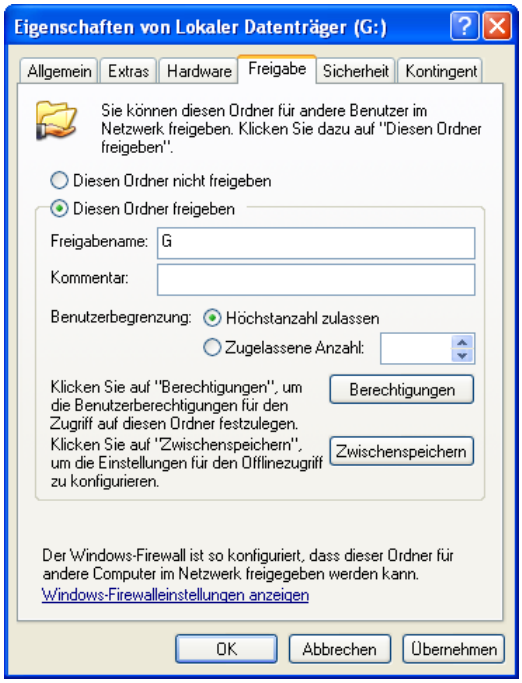
Eigenschaften von Lokaler Datenträger (G:)
Allgemein
Extras
Hardware
Freigabe
Sicherheit
Kontingent
Sie können diesen Ordner für andere Benutzer im Netzwerk freigeben. Klicken Sie dazu auf "Diesen Ordner freigeben".
Diesen Ordner nicht freigeben
Diesen Ordner freigeben
Freigabename: G
Kommentar:
Benutzerbegrenzung: Höchstanzahl zulassen
Zugelassene Anzahl:
Klicken Sie auf "Berechtigungen", um die Benutzerberechtigungen für den Zugriff auf diesen Ordner festzulegen.
Berechtigungen
Klicken Sie auf "Zwischenspeichern", um die Einstellungen für den Offlinezugriff zu konfigurieren.
Zwischenspeichern
Der Windows-Firewall ist so konfiguriert, dass dieser Ordner für andere Computer im Netzwerk freigegeben werden kann.
Windows-Firewalleinstellungen anzeigen
OK
Abbrechen
Übernehmen

Abbildung 73: Freigabe des Ordners in Windows XP

Tipp. Wenn in der Registerkarte **Freigabe** die Option **Diesen Ordner freigeben** nicht abgebildet wird, dann öffnen Sie in der **Systemsteuerung** die **Ordneroptionen** und deaktivieren Sie in der Registerkarte **Ansicht** das Kontrollkästchen **Einfache Dateifreigabe verwenden (empfohlen)**.

---

5 Klicken Sie auf **Übernehmen**, dann auf **OK**.

Nun ist für Ihren Container der allgemeine Zugriff eingerichtet. Wenn der Container eingebunden ist, können andere Benutzer mit Ihren geschützten Daten arbeiten, indem sie den von Ihnen erstellten Netzwerkordner öffnen. Damit der Zugang zum Container stets gewährleistet werden kann, sollte der Computer, auf dem sich der von Ihnen angelegte Netzwerkordner befindet, zugänglich sein. Wenn auf einem Computer abwechselnd gearbeitet

werden soll, verwenden Sie die Funktion **Benutzer wechseln**, wenn Sie mit Ihrer Arbeit fertig sind. Diese Funktion erlaubt es, einen Benutzerwechsel ohne Abmeldung im System durchzuführen, wodurch eine stetige Bereitschaft des Netzwerkordners gewährleistet wird.

Um die gemeinsame Nutzung geschützter Daten wieder zu blockieren, deaktivieren Sie die Freigabe des Laufwerks (s. Netzwerkzugang auf einen Container für die anderen Benutzer deaktivieren auf Seite 129).

Ebenso können Sie dazu den Container in ViPNet SafeDisk einfach trennen. Zum Aktivieren des allgemeinen Zugangs zum Container binden Sie diesen wieder ein (geben Sie bei der Einbindung das gleiche Laufwerk an, das zuvor freigegeben wurde).

Achtung! Nach einem Neustart des Computers muss der Netzwerkzugang zum Container neu eingestellt werden.

Netzwerkzugang auf einen Container für die anderen Benutzer deaktivieren

Zum Deaktivieren des Netzwerkzugangs auf den Container für andere Benutzer:

1. Deaktivieren Sie im Fenster **Erweiterte Freigabe** (s. Abbildung auf Seite 127) das Kontrollkästchen **Diesen Ordner freigeben**.
2. Klicken Sie auf **Übernehmen** und dann auf **OK**.

Achtung! Nach einem Neustart des Computers sollte die Konfiguration des Netzwerkzugriffs auf den Container erneut durchgeführt werden.

Auf dem Server gespeicherte Daten schützen

Sie können ViPNet SafeDisk auf einem Server in Ihrem Netzwerk installieren. Dadurch können Sie zusätzlich:

- Unternehmensdaten, die auf dem Server gespeichert sind, schützen;
- den gleichzeitigen Zugriff mehrerer Benutzer auf sensible Daten auf dem Server gewährleisten;
- vermeiden, dass ViPNet SafeDisk auf mehreren Arbeitsstationen installiert werden muss, wodurch die Ausgaben für Software beträchtlich reduziert werden können.

Zum Schützen von Unternehmensdaten, die auf dem Server gespeichert sind:

1. Installieren Sie ViPNet SafeDisk auf dem Server.
2. Machen Sie sich mit dem Kapitel Vorgehensweise beim Datenschutz (auf Seite 60) vertraut.
3. Erstellen Sie einen oder mehrere Container.
4. Binden Sie die erstellten Container ein und speichern Sie dort Daten ab, die für andere Benutzer zur Verfügung stehen sollen.
5. Aktivieren Sie mit Hilfe von Windows-Standardwerkzeugen die Freigabe für Laufwerke, die den neu erstellten Containern mit geschützten Daten zugeordnet sind (s. Netzwerkzugang auf einen Container für mehrere Benutzer ermöglichen auf Seite 124). Anschließend können Ihre Mitarbeiter auf die Container wie auf normale Netzlaufwerke zugreifen.
6. Deaktivieren Sie die Freigabe der Laufwerke (s. Netzwerkzugang auf einen Container für die anderen Benutzer deaktivieren auf Seite 129), um den allgemeinen Zugriff der Benutzer auf die sensiblen Daten wieder zu blockieren.

Der Einsatz von ViPNet SafeDisk auf einem Server unterscheidet sich kaum vom Einsatz des Programms auf einer einfachen Benutzer-Arbeitsstation. Mit Hilfe von ViPNet SafeDisk, das auf einem Server installiert ist, können Sie jederzeit folgende Aktionen durchführen:

- Eine Sicherungskopie der sensiblen Unternehmensdaten erstellen (s. Sicherungskopie der Containerschlüssel erstellen auf Seite 70).
- Einen sicheren Datenaustausch zwischen den Computern sicherstellen. Unternehmensdaten sollten insbesondere bei Übertragungen über ein offenes Netzwerk oder bei Transporten mit Hilfe eines Kuriers (unter Verwendung eines mobilen Datenträgers oder eines Notebooks) zuverlässig geschützt werden. Wenn das Notebook oder der Datenträger verloren oder gestohlen wird, bleibt der Datenzugang weiterhin geschützt, da die Daten verschlüsselt sind.
- Den allgemeinen Zugriff auf Unternehmensdaten im „Gefahr"-Modus unverzüglich blockieren (s. Zugang zu geschützten Daten sofort blockieren. „Gefahr"-Modus auf Seite 136).
- Vertrauliche Unternehmensdaten im „Extreme Gefahr"-Modus unverzüglich vernichten (s. Vertrauliche Daten vernichten. „Extreme Gefahr" Modus auf Seite 139).

Vertrauliche Daten mit Hilfe eines Kuriers oder über das Netzwerk übertragen

Beim Arbeiten mit Unternehmensdaten kann es manchmal erforderlich werden, sensible Informationen von einer Geschäftsstelle an eine andere zu übertragen. Wenn dabei das Notebook oder der Datenträger, die für den Transport verwendet werden, verloren gehen oder gestohlen werden, muss der Verlust von Daten unbedingt vermieden werden. Bei der Übertragung von Informationen über ungeschützte Netzwerkprotokolle (wie zum Beispiel FTP) können die Daten ebenfalls von Unbefugten abgefangen werden.

ViPNet SafeDisk ermöglicht es, Unternehmensdaten vor Verlusten während der Übertragung zu schützen.

Damit sensible Daten mit Hilfe eines Kuriers oder über das Netzwerk übertragen werden können:

1. Bereiten Sie die vertraulichen Daten für die Übertragung vor. Führen Sie dazu einen der folgenden Schritte aus:
   - Erstellen Sie eine Export-Datei des Containers (s. Container exportieren auf Seite 97).
   - Erstellen Sie eine Sicherungskopie der Containerschlüssel (s. Sicherungskopie der Containerschlüssel erstellen auf Seite 70) und kopieren diese zusammen mit der Container-Datei in einen Ordner.
2. Verschicken Sie die Daten über das Netzwerk oder übergeben diese an den Kurier.

Ausführliche Informationen dazu finden Sie im Kapitel Geschützte Daten exportieren und importieren (auf Seite 94).

9

Arbeit in einer potentiell unsicheren Umgebung

Vorbereitung für den Einsatz in einer unsicheren Umgebung: Vorgehensweise 134

Arbeit unter Kontrolle der Attentäter 135

Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus 136

Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus 139

Tastenkombinationen (Hotkeys) für den „Gefahr“ und „Extreme Gefahr“ Modus 142

Vorbereitung für den Einsatz in einer unsicheren Umgebung: Vorgehensweise

Damit Ihre vertraulichen Daten nicht in die Hände von Unbefugten geraten, sollten Sie alle Aufgaben aus der nachfolgenden Liste durchführen.

	Aufgabe	Textabschnitt
☐	Einen fiktiven Benutzer registrieren	Vorbereitung auf die Arbeit unter Kontrolle der Attentäter (auf Seite 135)
☐	Das Passwort für den fiktiven Benutzer merken	
☐	Sich unter dem fiktiven Benutzerkonto in ViPNet SafeDisk anmelden und Container mit unwichtigen Daten erstellen	Arbeit unter Kontrolle der Attentäter (auf Seite 135)
☐	Gefahr-Modus aktivieren	Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus (auf Seite 136)
☐	Modus „Extreme Gefahr“ aktivieren	Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus (auf Seite 139)
☐	Die Tastenkombination für die schnelle Trennung oder für sofortiges Löschen aller Container merken	Tastenkombinationen (Hotkeys) für den „Gefahr“ und „Extreme Gefahr“ Modus (auf Seite 142)

Tipp. Es wird empfohlen, die Liste auszudrucken und die einzelnen Punkte nach ihrer Abarbeitung zu markieren.

Arbeit unter Kontrolle der Attentäter

In ViPNet SafeDisk können Sie Ihre Daten schützen auch wenn Sie sich unter der Kontrolle der Attentäter befinden.

Vorbereitung auf die Arbeit unter Kontrolle der Attentäter

1. Registrieren Sie einen neuen Benutzer (s. Zugriff auf die geschützten Daten verwalten. Neuen Benutzer registrieren auf Seite 119). Sie können dieses Konto als fiktiven Benutzer verwenden.
2. Melden Sie sich unter dem fiktiven Benutzerkonto an und erstellen Sie ein Container (s. Container erstellen auf Seite 61).
3. Binden Sie den Container ein (s. Container einbinden auf Seite 74).
4. Speichern Sie im Container unwichtige Daten, welche Ihre sensiblen Daten imitieren.
5. Merken Sie sich das Passwort des fiktiven Benutzers.

Arbeit unter Kontrolle der Attentäter

Wenn Sie festgestellt haben, dass Sie unter Kontrolle der Attentäter arbeiten:

1. Starten Sie ViPNet SafeDisk (s. ViPNet SafeDisk starten auf Seite 29).
2. Geben Sie das Passwort des fiktiven Benutzers ein.
3. Binden Sie den Container mit fiktiven Daten ein (s. Einen früher erstellen Container einbinden auf Seite 77).

   Für eine gewisse Zeit besteht jetz die Möglichkeit, dass nicht erkannt wird, ob es sich um die echten oder um die fiktiven Daten handelt.

Zugang zu geschützten Daten sofort blockieren. „Gefahr“-Modus

Wenn Sie der Meinung sind, dass die sich in Ihrer Umgebung befindlichen Außenstehenden eine Gefahr darstellen könnten, oder wenn Sie wissen, dass sich Unbefugte annähern, können Sie wie folgt vorgehen:

1 Führen Sie im Hauptfenster von ViPNet SafeDisk rechtzeitig eine der folgenden Aktionen aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Gefahr** .
- Wählen Sie im Menü **Sicherheit** den Eintrag **„Gefahr“-Modus**.
- Wählen Sie im Menü **SafeDisk** den Punkt **Einstellungen**, öffnen sie im Fenster **Einstellungen** die Registerkarte **„Gefahr“ Modus** und aktivieren Sie das Kontrollkästchen „Gefahr“ Modus. Klicken Sie anschließend auf **Übernehmen**.

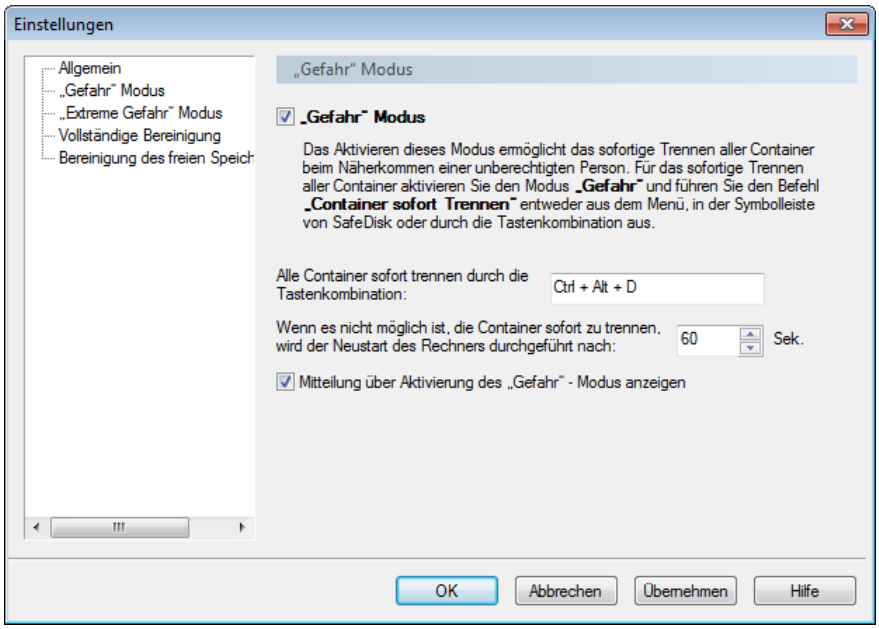
Einstellungen
Allgemein
„Gefahr" Modus
„Extreme Gefahr" Modus
Vollständige Bereinigung
Bereinigung des freien Speich
„Gefahr" Modus
„Gefahr" Modus
Das Aktivieren dieses Modus ermöglicht das sofortige Trennen aller Container beim Näherkommen einer unberechtigten Person. Für das sofortige Trennen aller Container aktivieren Sie den Modus „Gefahr" und führen Sie den Befehl „Container sofort Trennen" entweder aus dem Menü, in der Symbolleiste von SafeDisk oder durch die Tastenkombination aus.
Alle Container sofort trennen durch die Tastenkombination:
Ctrl + Alt + D
Wenn es nicht möglich ist, die Container sofort zu trennen, wird der Neustart des Rechners durchgeführt nach:
60
Sek.
Mitteilung über Aktivierung des „Gefahr" - Modus anzeigen
OK
Abbrechen
Übernehmen
Hilfe

Abbildung 74: „Gefahr“ Modus aktivieren

„Gefahr“ Modus wird nun aktiviert.

Tipp. Wenn Sie nicht möchten, dass vom Programm Warnmeldungen über die Aktivierung des „Gefahr“- Modus eingeblendet werden, dann deaktivieren Sie entweder auf der Registerkarte **„Gefahr“ Modus** das Kontrollkästchen **Mitteilung über Aktivierung des „Gefahr“-Modus anzeigen** oder aktivieren Sie im Meldungsfenster „**Gefahr“-Modus aktivieren** das Kontrollkästchen **Dieses Fenster nicht mehr anzeigen**.

2 Wenn sich Unbefugte Ihrem Computer annähern, führen Sie eine der folgenden Aktionen aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Alle Container sofort trennen** .
- Wählen Sie im Menü **Sicherheit** den Befehl **Alle Container sofort trennen**.
- Drücken Sie die Tastenkombination **Strg**+**Alt**+**D** (standardmäßig eingestellte Kombination).

Tipp. Zum Ändern des Hotkey-Tastaturbefehls klicken Sie in der Registerkarte **„Gefahr“ Modus** (s. Abbildung auf Seite 136) in das Eingabefeld **Alle Container sofort trennen durch die Tastenkombination** und drücken die Tastenkombination, die Sie einstellen wollen. Klicken Sie anschließend auf **Übernehmen**.

Alle Container werden sofort getrennt, der Zugang zu in diesen Containern gespeicherten Daten wird blockiert. Windows-Laufwerke, die den eingebundenen Containern zugeordnet sind, werden in der Ordnerübersicht Ihres Computers nicht mehr angezeigt. Das Programmfenster von ViPNet SafeDisk wird geschlossen, das Programmsymbol im Infobereich der Taskleiste wird ausgeblendet. Es bleiben keine Spuren übrig, die von Ihrer Arbeit mit vertraulichen Daten zeugen könnten.

Wenn ViPNet SafeDisk es nicht schafft, innerhalb der angegebenen Zeit (standardmäßig 60 Sekunden) alle Container zu trennen, dann:

- werden alle eingebundenen Container zwangsweise getrennt,
- werden alle Anwendungen, die vom Benutzer gestartet wurden, geschlossen,
- wird die Arbeitssitzung des aktuellen Benutzers beendet.

Zum Ändern dieses Zeitintervalls:

1. Wählen Sie im Menü **SafeDisk** den Eintrag **Einstellungen**.
2. Öffnen Sie im Fenster **Einstellungen** die Registerkarte **„Gefahr“ Modus** (s. Abbildung auf Seite 136).
3. Geben Sie in der Registerkarte **„Gefahr“ Modus** im Feld **Wenn es nicht möglich ist, die Container sofort zu trennen, wird der Neustart des Rechners durchgeführt** den neuen Wert für das Zeitintervall in Sekunden ein.
4. Klicken Sie auf **Übernehmen**.

Zum Deaktivieren des „Gefahr“ Modus:

1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Gefahr** .
2. Wählen Sie im Menü **Sicherheit** den Eintrag **„Gefahr“-Modu**s.
3. Deaktivieren Sie im Fenster **Einstellungen** in der Registerkarte **„Gefahr“ Modus** (s. Abbildung auf Seite 136) das Kontrollkästchen **„Gefahr“ Modus** und klicken anschließend auf **Übernehmen**.

Vertrauliche Daten vernichten. „Extreme Gefahr“ Modus

Der Modus „Extreme Gefahr“ ermöglicht es, alle in den Containern enthaltenen vertraulichen Daten schnell zu vernichten. Dies kann dann von Nutzen sein, wenn sich Ihnen Unbefugte annähern, und Sie keinen anderen Ausweg sehen, als alle sensiblen Informationen schnell zu löschen.

Achtung! Verwenden Sie den Modus „Extreme Gefahr“ nur in Ausnahmefällen. Container, die in diesem Modus gelöscht wurden, können nicht mehr wiederhergestellt werden.

Beim Löschen der Container im Modus „Extreme Gefahr“ werden die Containerschlüssel aller Benutzer vernichtet, und die in den Containern gespeicherten Daten gehen verloren.

Zum unverzüglichen Vernichten von vertraulichen Daten:

1. Führen Sie im Hauptfenster von ViPNet SafeDisk rechtzeitig eine der folgenden Aktionen aus:
   - Klicken Sie in der Symbolleiste auf die Schaltfläche **Extreme Gefahr** .
   - Wählen Sie im Menü Sicherheit den Punkt **„Extreme Gefahr“-Modus**.

- Wählen Sie im Menü **SafeDisk** den Punkt **Einstellungen**, öffnen im Fenster **Einstellungen** die Registerkarte **„Extreme Gefahr“ Modus** und aktivieren das Kontrollkästchen **„Extreme Gefahr“ Modus**. Klicken Sie anschließend auf **Übernehmen**.

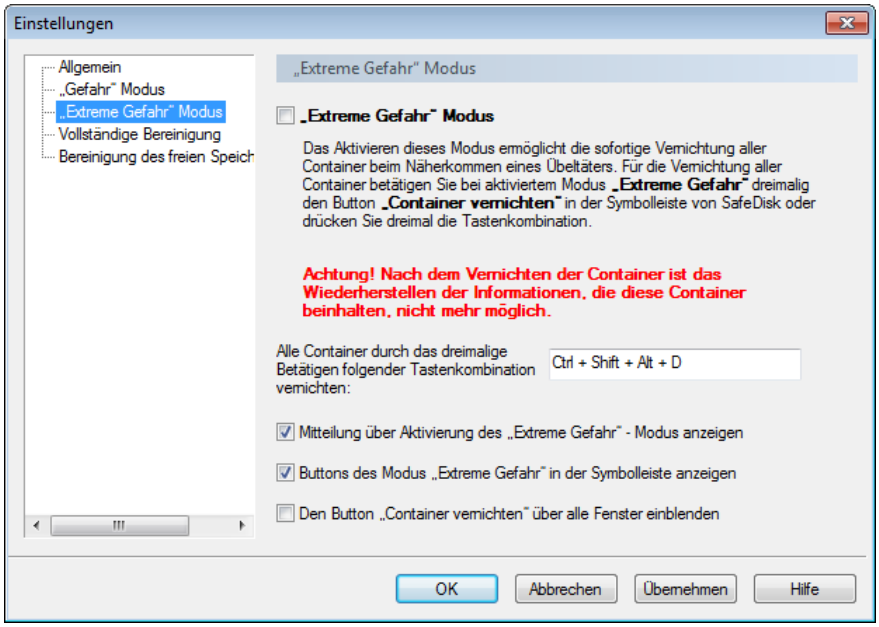
Einstellungen
Allgemein
„Gefahr“ Modus
„Extreme Gefahr“ Modus
Vollständige Bereinigung
Bereinigung des freien Speich
„Extreme Gefahr“ Modus
„Extreme Gefahr“ Modus
Das Aktivieren dieses Modus ermöglicht die sofortige Vernichtung aller Container beim Näherkommen eines Übeltäters. Für die Vernichtung aller Container betätigen Sie bei aktiviertem Modus „Extreme Gefahr“ dreimalig den Button „Container vernichten“ in der Symbolleiste von SafeDisk oder drücken Sie dreimal die Tastenkombination.
Achtung! Nach dem Vernichten der Container ist das Wiederherstellen der Informationen, die diese Container beinhalten, nicht mehr möglich.
Alle Container durch das dreimalige Betätigen folgender Tastenkombination vernichten:
Ctrl + Shift + Alt + D
Mitteilung über Aktivierung des „Extreme Gefahr“ - Modus anzeigen
Buttons des Modus „Extreme Gefahr“ in der Symbolleiste anzeigen
Den Button „Container vernichten“ über alle Fenster einblenden
OK
Abbrechen
Übernehmen
Hilfe

Abbildung 75: „Extreme Gefahr“-Modus aktivieren

Tipp. Wenn Sie nicht möchten, dass vom Programm Warnmeldungen über die Aktivierung des „Extreme Gefahr“- Modus eingeblendet werden, deaktivieren Sie entweder auf der Registerkarte **„Extreme Gefahr“ Modus** das Kontrollkästchen **Mitteilung über Aktivierung des „Extreme Gefahr“-Modus anzeigen** oder aktivieren Sie im Meldungsfenster **„Extreme Gefahr“-Modus aktivieren** das Kontrollkästchen **Dieses Fenster nicht mehr anzeigen**.

---

2 Zum sofortigen Vernichten vertraulicher Daten klicken Sie in der Symbolleiste dreimal auf die Schaltfläche **Alle Container vernichten** oder drücken dreimal in Folge die Hotkey-Tastenkombination **Strg+Umschalt+Alt+D**.

Tipp. Zum Ändern des Hotkey-Tastaturbefehls klicken Sie in der Registerkarte **„Extreme Gefahr“ Modus** (s. Abbildung auf Seite 140) in das Eingabefeld **Alle Container durch das dreimalige Betätigen folgender Tastenkombination vernichten** und drücken die Tastenkombination, die Sie einstellen wollen. Klicken Sie anschließend auf **Übernehmen**.

Alle Container, Containerschlüssel und Sicherungskopien der Konfiguration werden sofort vernichtet. Das Programmfenster von ViPNet SafeDisk wird geschlossen, das Symbol im Infobereich der Taskleiste wird ausgeblendet. Wenn ViPNet SafeDisk es nicht schafft, innerhalb der angegebenen Zeit (standardmäßig 60 Sekunden) alle Container zu trennen, dann:

- werden alle eingebundenen Container zwangsweise getrennt,
- werden alle Anwendungen, die vom Benutzer gestartet wurden, geschlossen,
- wird die Arbeitssitzung des aktuellen Benutzers beendet.

Beim nächsten Programmstart wird die Container-Liste leer.

Sie können die Schaltflächen des „Extreme Gefahr“ Modus von der ViPNet SafeDisk Symbolleiste entfernen. Dazu:

1. Deaktivieren Sie im Fenster **Einstellungen** in der Registerkarte **„Extreme Gefahr“ Modus** (s. Abbildung auf Seite 140) das Kontrollkästchen **Buttons des Modus „Extreme Gefahr“ in der Symbolleiste anzeigen**.
2. Klicken Sie auf **Übernehmen**.

Sie können zusätzlich die halbtransparente Schaltfläche **Alle Container vernichten** im rechten unteren Bereich Ihres Desktops aktivieren. Führen Sie dafür die folgenden Schritte durch:

1. Aktivieren Sie Im Fenster **Einstellungen** in der Registerkarte **„Extreme Gefahr“ Modus** (s. Abbildung auf Seite 140) das Kontrollkästchen **Den Button „Container vernichten“ über alle Fenster einblenden**.
2. Klicken Sie auf **Übernehmen**.

Zum Deaktivieren des „Extreme Gefahr“ Modus führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Extreme Gefahr** .
- Wählen Sie im Menü **Sicherheit** den Eintrag **„Extreme Gefahr“-Modus**.
- Deaktivieren Sie im Fenster **Einstellungen** in der Registerkarte **„Extreme Gefahr“ Modus** (s. Abbildung auf Seite 140) das Kontrollkästchen **„Extreme Gefahr“ Modus** und klicken anschließend auf **Übernehmen**.

Tastenkombinationen (Hotkeys) für den „Gefahr“ und „Extreme Gefahr“ Modus

Strg+Alt+D – drücken Sie diese Tastenkombination, um unverzüglich alle Container zu trennen (Modus „Gefahr“ muss dabei aktiviert sein).

Strg+Umschalt+Alt+D – drücken Sie diese Tastenkombination dreimal in Folge, um unverzüglich alle Ihre Container zu vernichten (Modus „Extreme Gefahr“ muss dabei aktiviert sein).

10

Spurenbeseitigung bei der Arbeit mit privaten Daten

Warum die Datenbereinigung notwendig ist	144
Vorgehensweise beim Bereinigen von Datenspuren	146
Bereinigung von Datenspuren: Reihenfolge der Schritte	148
Datenspuren in Windows bereinigen	149
Datenspuren im Internet Explorer bereinigen	154
Vollständige Bereinigung	157
Bereinigung über die Befehlszeile starten	160

Warum die Datenbereinigung notwendig ist

Das Betriebssystem Windows ermöglicht es, Dateien wiederherzustellen, falls Sie diese aus Versehen gelöscht, den Papierkorb bereinigt oder die Dateien mit Hilfe der Tastenkombination **Umschalt+Entf** entfernt haben. Die Wiederherstellung der Daten ist auch dann möglich, wenn das Laufwerk formatiert wurde oder wenn die Festplatte ausgefallen ist und alle Daten als verloren gemeldet wurden.

Wenn Sie eine Datei durch Anwendung von Standardmethoden löschen, bleiben die Daten physikalisch auf der Festplatte erhalten. Das Betriebssystem vermerkt lediglich die Datei als gelöscht, indem es den Dateinamen ändert. Später können an der Stelle der Datei andere Daten gespeichert werden.

Nach der Formatierung der Festplatte bleibt eine zuvor erstellte Sicherungskopie übrig. Wenn es zum Ausfall der Festplatte kommt, können die Daten mit Hilfe physikalischer Methoden wiederhergestellt werden.

Das bedeutet, dass Sie Ihre privaten Daten ohne Anwendung zusätzlicher Werkzeuge nicht sicher und zuverlässig löschen können. Im Lieferumfang von ViPNet SafeDisk ist die Utility Clean.exe enthalten, die für das vollständige Löschen von ungeschützten Daten sorgt.

Hinweis. Daten, die mit Hilfe von ViPNet SafeDisk geschützt sind, werden immer zuverlässig bereinigt

Das sichere Löschen von Daten kann in folgenden Situationen erforderlich sein:

- Sie haben einen Container mit der Schlüssel-Datei geschützt. Danach wurde der Container gelöscht. Die Schlüssel-Datei ist erhalten geblieben, sie beinhaltet sensible Daten und muss sicher gelöscht werden.
- Sie haben im Programm MS Word an einem sensiblen Dokument gearbeitet. Auch wenn Sie das Dokument in einem ViPNet SafeDisk-Container aufbewahren, bleiben im Betriebssystem Windows Informationen darüber, welche Datei wann, von wem und an welchem Speicherort geöffnet wurde. Aus Sicherheitsgründen sollten Sie diese Informationsspuren bereinigen.

- Sie haben eine Transaktion im Internet durchgeführt, bei welcher Sie Ihre persönlichen und finanziellen Daten verwendet haben. Die Spuren dieses Vorgangs bleiben in Cookie-Dateien und in temporären Internet-Dateien erhalten. Diese Daten sollten aus Selbstschutzgründen vollständig gelöscht werden.

- Sie haben einen neuen Computer gekauft und wollen den alten Rechner verkaufen. Sie haben die Festplatte des Rechners mit Hilfe herkömmlicher Werkzeuge von Windows formatiert, um mögliche Spuren vertraulicher Daten, mit denen Sie auf dem alten Computer gearbeitet haben, zu entfernen. Es gibt jedoch Verfahren, die es ermöglichen, die Daten auf einer formatierten Festplatte wiederherzustellen. Um sicherzustellen, dass Ihre privaten Daten nicht nachträglich weiterverwendet werden, sollten Sie mit Hilfe der Funktionalität von ViPNet SafeDisk den freien Speicherplatz auf den Laufwerken regelmäßig bereinigen.

Vorgehensweise beim Bereinigen von Datenspuren

Wenn Sie mit unterschiedlichen Dateien gearbeitet, Texte kopiert, Dateien aus einem Ordner in einen anderen verschoben oder Dateien mit Hilfe von Standardwerkzeugen gelöscht haben, sollten Sie regelmäßig dafür sorgen, die verbliebenen Datenfragmente sicher und vollständig zu bereinigen.

Mit Hilfe der Bereinigungsfunktionalität von ViPNet SafeDisk können Sie Ihre Arbeitsspuren zuverlässig löschen. Zuerst müssen Sie die zu bereinigenden Objekte bestimmen. Sie können Ihre Arbeitsspuren im Betriebssystem Windows und im Internet Explorer bereinigen.

Mit Hilfe von ViPNet SafeDisk können im Betriebssystem Windows folgende Objekte bereinigt werden:

- Zuletzt verwendete Dokumente.
- Temporäre Dateien.
- Papierkorb.
- Freier Speicherplatz auf den Laufwerken, auf denen Daten vor ihrer Übertragung in ViPNet SafeDisk-Container gespeichert waren.

Weitere Details zur Handhabung der aufgezählten Objekte finden Sie im Kapitel Datenspuren in Windows bereinigen (auf Seite 149).

Ebenso können folgende Internet Explorer Objekte bereinigt werden:

- Verlauf.
- Temporäre Internetdateien.
- Cookie-Dateien.

Weitere Details zur Handhabung der aufgezählten Objekte finden Sie im Kapitel Datenspuren im Internet Explorer bereinigen (auf Seite 154).

ViPNet SafeDisk ermöglicht es, mit Hilfe der Funktion **Vollständige Bereinigung** (s. Vollständige Bereinigung auf Seite 157) ein vollständiges Entfernen aller Spuren vertraulicher Daten zeitgleich durchzuführen.

Wenn Sie ein erfahrener Benutzer oder Programmierer sind, können Sie die Utility Clean.exe (s. Bereinigung über die Befehlszeile starten auf Seite 160) verwenden, um die vollständige Bereinigung von Datenspuren mit Hilfe eines Kommandozeilenbefehls durchzuführen.

Bereinigung von Datenspuren: Reihenfolge der Schritte

Wenn Sie sicher sein wollen, dass Sie die Datenspuren sicher bereinigt haben, führen Sie alle Schritte aus der nachfolgenden Tabelle durch.

	Aufgabe	Verweis
☐	Liste der zuletzt verwendeten Dokumente regelmäßig löschen	Liste zuletzt verwendeter Dateien löschen (auf Seite 149)
☐	Temporäre Dateien regelmäßig löschen	Temporäre Dateien löschen (auf Seite 149)
☐	Papierkorb regelmäßig bereinigen	Papierkorb bereinigen (auf Seite 150)
☐	Spuren verschobener oder gelöschter ungeschützter Dateien regelmäßig bereinigen	Sicheres Löschen ungeschützter Dateien (auf Seite 150)
☐	Freien Speicherplatz auf der Festplatte regelmäßig bereinigen	Freien Speicherplatz auf Laufwerken bereinigen (auf Seite 151)
☐	Browserverlauf regelmäßig löschen	Datenspuren im Internet Explorer bereinigen (auf Seite 154)
☐	Temporäre Internetdateien regelmäßig entfernen	Temporäre Internetdateien löschen (auf Seite 154)
☐	Cookie-Dateien regelmäßig bereinigen	Cookies bereinigen (auf Seite 155)

Tipp. Es wird empfohlen, die Liste auszudrucken und die einzelnen Punkte nach ihrer Abarbeitung zu markieren.

Datenspuren in Windows bereinigen

Liste zuletzt verwendeter Dateien löschen

Windows ermöglicht eine schnellere Suche nach vor Kurzem geöffneten Dokumenten, indem Verweise auf diese Dokumente im Ordner **Zuletzt verwendete Dokumente** gespeichert werden. Dieser Ordner kann über das Menü **Start** aufgerufen werden. Anhand dieser Verweise können Unbefugte Informationen über die Existenz sensibler Daten erhalten. Aus Sicherheitsgründen sollte der Ordner **Zuletzt verwendete Dokumente** regelmäßig geleert werden.

ViPNet SafeDisk entfernt auf eine sichere Art und Weise Links auf kürzlich geöffnete Dokumente aus den nachfolgenden Ordnern:

- `C:\Users\Benutzername\AppData\Roaming\Microsoft\Windows\Recent` (in Vista und späteren Versionen von Windows).
- `C:\Users\Benutzername\AppData\Roaming\Microsoft\Office\Recent` (in Vista und späteren Versionen von Windows).
- `C:\Documents and Settings\Benutzername\Recent` (in Windows XP).

Zum Bereinigen des Ordners **Zuletzt verwendete Dokumente**:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** auf den Eintrag **Windows** und klicken anschließend auf **Windows Arbeitsverlauf**.
2. Dadurch werden alle Verweise auf kürzlich geöffnete Dokumente gelöscht.

Tipp. Sie können ViPNet SafeDisk so einstellen, dass die Liste der zuletzt verwendeten Dokumente automatisch beim Beenden jeder Arbeitssitzung bereinigt wird (s. Parameter von ViPNet SafeDisk einstellen auf Seite 92).

Temporäre Dateien löschen

Viele Windows-Anwendungen erstellen beim Öffnen von Dokumenten temporäre Dateien. Diese Dateien können eine vollständige Kopie der Originaldatei sowie weitere System- und Zusatzinformationen enthalten. In der Regel werden temporäre Dateien automatisch gelöscht,

wenn die Originaldatei geschlossen wird. In einigen Fällen werden neu angelegte temporäre Dateien jedoch nicht entfernt. Diese „vergessenen“ temporären Dateien, die vertrauliche Daten enthalten, können eine ernsthafte Gefahr für die Informationssicherheit des Unternehmens darstellen. Deswegen müssen bei Handhabung sensibler Daten die von unterschiedlichen Anwendungen zurückgelassenen temporären Dateien regelmäßig auf eine sichere Art und Weise gelöscht werden.

ViPNet SafeDisk entfernt auf sichere Art und Weise temporäre Dateien aus den nachfolgenden Ordnern:

- `C:\WINDOWS\Temp` (oder ein anderer Ordner, der im System als Standardordner für temporäre Dateien definiert ist).
- `C:\Documents and Settings\Benutzername\Local Settings\Temp` (in Windows XP:).
- `C:\Users\Benutzername\AppData\Local\Temp` (in Vista und späteren Versionen von Windows).

Zum Löschen von temporären Dateien:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** auf den Eintrag **Windows** und klicken anschließend auf **Temporäre Dateien**.
2. Dadurch werden alle temporären Dateien, die von unterschiedlichen Anwendungen angelegt wurden, sicher gelöscht.

Papierkorb bereinigen

Dateien, die mit herkömmlichen Mitteln gelöscht wurden, werden in den **Papierkorb** verschoben und können leicht wiederhergestellt werden. Damit ein Wiederherstellen gelöschter Dateien aus dem **Papierkorb** verhindert wird, müssen Sie den **Papierkorb** zuverlässig bereinigen.

Zum Bereinigen des **Papierkorbs**:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** auf den Eintrag **Windows** und klicken anschließend auf **Papierkorb**.
2. Dadurch wird der gesamte Inhalt von **Papierkorb** sicher gelöscht.

Sicheres Löschen ungeschützter Dateien

Bevor Sie ViPNet SafeDisk auf Ihrem Computer installiert haben, wurden vertrauliche Daten ungeschützt auf der Festplatte gespeichert. Wie Sie wissen, kann diese Art der Speicherung

nicht den benötigten Umfang an Informationssicherheit gewährleisten. Sogar nach dem Löschen der Dateien von der Festplatte und dem anschließenden Leeren des Papierkorbs können Daten mit Hilfe spezieller Werkzeuge oder physikalischer Eingriffe wiederhergestellt werden.

Nach der Installation von ViPNet SafeDisk haben Sie alle Dateien, die sensible Informationen beinhalten, in geschützte Container verschoben. Diese Dateien können aber immer noch auf der Festplatte leicht wiederhergestellt werden. Um diese Gefahrenquelle zu beseitigen, sollten die Dateien nach dem Verschieben vollständig und sicher von der Festplatte entfernt werden.

Zum sicheren Löschen von ungeschützten Dateien führen Sie einen der folgenden Schritte aus:

- Löschen Sie die Dateien auf eine sichere Art und Weise (s. Dateien sicher löschen auf Seite 151).
- Wenn Sie die Dateien mit Hilfe herkömmlicher Mittel von Windows bereits gelöscht haben, verwenden Sie ViPNet SafeDisk dazu, freien Speicherplatz auf der Festplatte zu bereinigen (s. Freien Speicherplatz auf Laufwerken bereinigen auf Seite 151).

Dateien sicher löschen

Zum sicheren Löschen von Dateien:

1. Markieren Sie die betroffene Datei im ungeschützten Ordner.
2. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie im Kontextmenü den Eintrag **Sicheres Löschen** (in Windows 7 und in früheren Windows-Versionen als Vista können Sie auch in der Ordnerübersicht im Menü **Datei** den Befehl **Sicheres Löschen** auswählen).
3. Klicken Sie im Fenster **Sicheres Löschen** bestätigen auf **Ja**.

Freien Speicherplatz auf Laufwerken bereinigen

Zum Bereinigen des freien Festplattenspeichers:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** auf den Eintrag **Windows** und klicken Sie anschließend auf **Freier Speicherplatz**. Es wird der Assistent **Sicheres Löschen** gestartet.
2. Aktivieren Sie auf der Seite **Freier Speicherplatz auf den Laufwerken** die Kontrollkästchen neben den Laufwerken, die Sie bereinigen möchten, und klicken Sie auf **Weiter**.

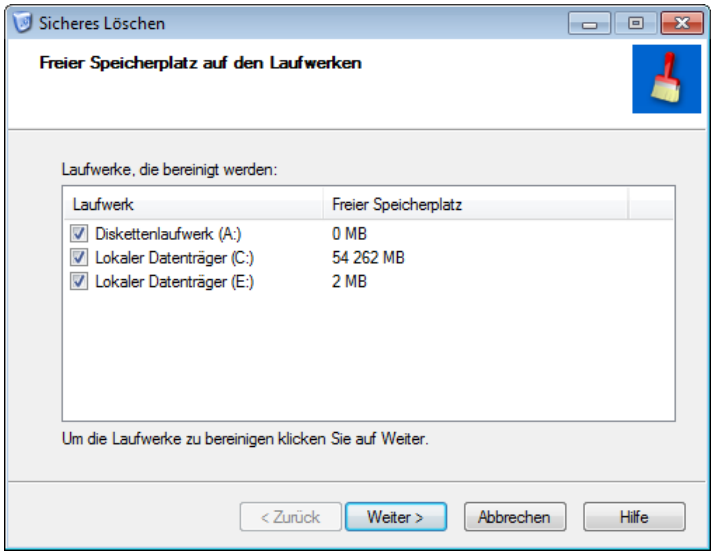

Abbildung 76: Freien Speicherplatz auf den Laufwerken bereinigen

3 Warten Sie, bis der Bereinigungsvorgang abgeschlossen ist.

4 Klicken Sie auf der Seite **Bereinigung wird abgeschlossen** auf die Schaltfläche **Fertig**.

Laufwerke für standardmäßige Bereinigung des freien Speicherplatzes einstellen

Zum Einstellen von Laufwerken für eine automatische Bereinigung des freien Speicherplatzes:

1 Wählen Sie im Hauptfenster von ViPNet SafeDisk im Menü **SafeDisk** den Eintrag **Einstellungen**.

2 Öffnen Sie im Fenster **Einstellungen** die Registerkarte **Bereinigung des freien Speicherplatzes**.

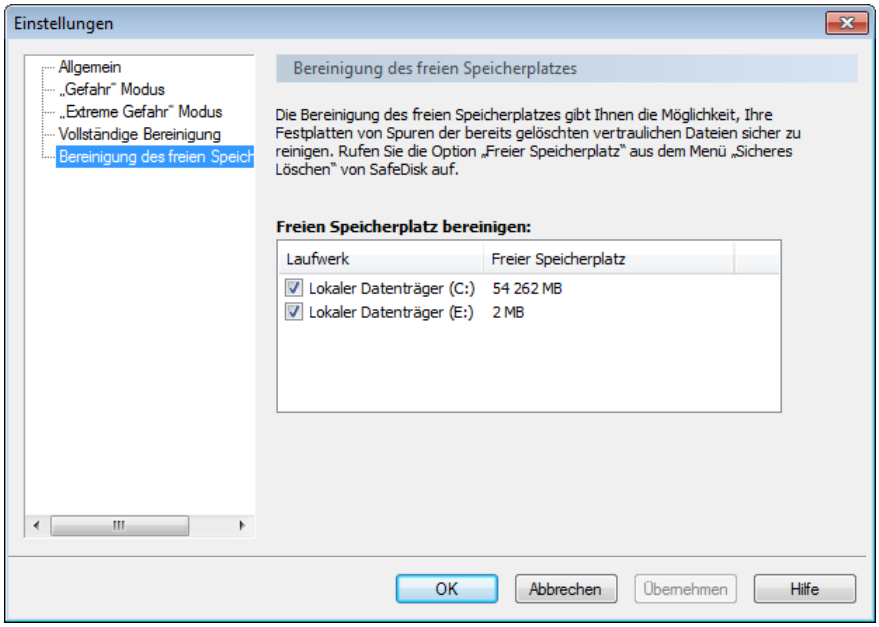
Einstellungen
Allgemein
„Gefahr" Modus
„Extreme Gefahr" Modus
Vollständige Bereinigung
Bereinigung des freien Speich
Bereinigung des freien Speicherplatzes
Die Bereinigung des freien Speicherplatzes gibt Ihnen die Möglichkeit, Ihre Festplatten von Spuren der bereits gelöschten vertraulichen Dateien sicher zu reinigen. Rufen Sie die Option „Freier Speicherplatz" aus dem Menü „Sicheres Löschen" von SafeDisk auf.
Freien Speicherplatz bereinigen:
Laufwerk
Freier Speicherplatz
Lokaler Datenträger (C:) 54 262 MB
Lokaler Datenträger (E:) 2 MB
OK
Abbrechen
Übernehmen
Hilfe

Abbildung 77: Laufwerke für Speicherbereinigung auswählen

3 Aktivieren Sie in der Liste **Freien Speicherplatz bereinigen** die Kontrollkästchen neben den Laufwerken, die Sie standardmäßig bereinigen möchten.

4 Klicken Sie auf **Übernehmen** und dann auf **OK**.

Datenspuren im Internet Explorer bereinigen

Achtung! Die Bereinigung des Browserverlaufs, der temporären Internetdateien und Cookies wird nur für den Browser MS Internet Explorer durchgeführt. Die Bereinigung der Browser anderer Hersteller wird in nachfolgenden Versionen von ViPNet SafeDisk implementiert.

Browserverlauf leeren

Wenn Sie sich Webseiten anzeigen lassen, speichert Internet Explorer Informationen über die von Ihnen besuchten Seiten ab (standardmäßig wird der Browserverlauf der letzten 3 Wochen gespeichert). Die Liste der besuchten Webseiten hilft dabei, schneller zu den früher aufgerufenen Seiten zurückzukehren. Wenn Sie aber nicht wollen, dass diese Informationen für Andere zugänglich sind, sollten Sie den Browserverlauf regelmäßig löschen.

Der Internet Explorer Browserverlauf wird in folgenden Ordnern gespeichert:

- `C:\Documents and Settings\Benutzername\Local Settings\History` (in Windows XP);
- `C:\Users\Benutzername\AppData\Local\Microsoft\Windows\History` (in Vista und späteren Versionen von Windows)

Zum Bereinigen des Browserverlaufs vom Internet Explorer:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** auf den Eintrag **Internet Explorer** und klicken anschließend auf **Verlauf**.
2. Dadurch werden alle Informationen über die von Ihnen besuchten Webseiten gelöscht.

Temporäre Internetdateien löschen

Beim Arbeiten mit Webseiten speichert Internet Explorer alle Daten ab, die er aus dem Internet erhält. Das kann dann von Nutzen sein, wenn für den Internetzugang eine langsame Modem-Verbindung verwendet wird, da so die Ladegeschwindigkeit von Web-Inhalten gesteigert

werden kann. Wenn Sie aber nicht wollen, dass diese Daten für Andere zugänglich werden, sollten Sie die temporären Internetdateien regelmäßig löschen.

Internet Explorer speichert die temporäre Dateien in folgenden Ordnern ab:

- `C:\Documents and Settings\Benutzername\Local Settings\Temporary Internet Files` (in Windows XP).
- `C:\Users\Benutzername\AppData\Local\Microsoft\Windows\Temporary Internet Files` (in Vista und späteren Versionen von Windows).

Zum Löschen temporärer Internetdateien:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** auf den Eintrag **Internet Explorer** und klicken anschließend auf **Temporäre Dateien**.
2. Dadurch werden alle temporären Internetdateien auf sichere Art und Weise gelöscht.

Cookies bereinigen

Eine Cookie-Datei stelle eine Textdatei dar, die vom Internet-Browser auf dem Computer abgespeichert wird. In diesen Dateien können Inhalte von Warenkörben eines Online-Shops, Namen und Passwörter von Benutzerkonten unterschiedlicher Webseiten sowie andere private Daten abgelegt werden. Um diese Daten unzugänglich zu machen, müssen die Cookie-Dateien gelöscht werden.

Achtung! Damit Cookie-Dateien erfolgreich gelöscht werden können, muss Internet Explorer zuvor beendet werden.

Internet Explorer speichert die Cookie-Dateien in den folgenden Ordnern ab:

- In Windows XP:
  - `C:\Documents and Settings\Benutzername\Cookies.`
  - `C:\Documents and Settings\Benutzername\Local Settings\Temporary Internet Files.`
- In Windows Vista und späteren Windows-Versionen:
  - `C:\Users\Benutzername\AppData\Roaming\Microsoft\Windows\Cookies.`
  - `C:\Users\Benutzername\AppData\Local\Microsoft\Windows\Temporary Internet Files.`

Zum Löschen von Cookie-Dateien:

1. Zeigen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** auf den Eintrag **Internet Explorer** und klicken anschließend auf **Cookies**.
2. Dadurch werden alle Cookie-Dateien, die vertrauliche Daten enthalten könnten, auf sichere Art und Weise gelöscht.

Vollständige Bereinigung

Wenn nötig, können Sie gleichzeitig mehrere Typen von Objekten bereinigen, um alle Spuren der Arbeit mit vertraulichen Daten zu vernichten. Dazu:

1. Wählen Sie im Hauptfenster von ViPNet SafeDisk im Menü **Sicheres Löschen** den Eintrag **Vollständige Bereinigung**. Es wird der Assistent **Vollständige Bereinigung** gestartet.

2. Aktivieren Sie auf der Seite **Vollständige Bereinigung** in der Liste **Bereinigen** die Kontrollkästchen neben den Objekten, die Sie bereinigen möchten.

   Klicken Sie auf **Weiter**.

Abbildung 78: Assistent für die vollständige Bereinigung

3. Aktivieren Sie auf der Seite **Freier Speicherplatz** auf den Laufwerken das Kontrollkästchen **Freien Speicherplatz auf Laufwerken bereinigen**, wenn Sie den freien Speicherplatz auf der Festplatte von Spuren gelöschter oder verschobener sensibler Dokumente bereinigen möchten.

   Aktivieren Sie in der Liste **Laufwerke, die bereinigt werden** die Kontrollkästchen neben den Laufwerken, die Sie bereinigen möchten. Klicken Sie anschließend auf **Weiter**.

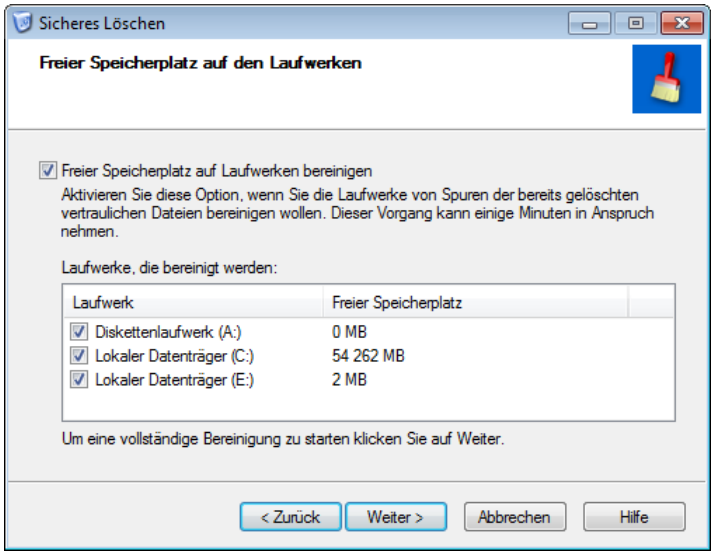
Sicheres Löschen
Freier Speicherplatz auf den Laufwerken
Freier Speicherplatz auf Laufwerken bereinigen
Aktivieren Sie diese Option, wenn Sie die Laufwerke von Spuren der bereits gelöschten vertraulichen Dateien bereinigen wollen. Dieser Vorgang kann einige Minuten in Anspruch nehmen.
Laufwerke, die bereinigt werden:
Laufwerk
Freier Speicherplatz
Diskettenlaufwerk (A:)
0 MB
Lokaler Datenträger (C:)
54 262 MB
Lokaler Datenträger (E:)
2 MB
Um eine vollständige Bereinigung zu starten klicken Sie auf Weiter.
< Zurück
Weiter >
Abbrechen
Hilfe

Abbildung 79: Laufwerke für Bereinigung des freien Speicherplatzes auswählen

4 Auf der Seite **Bereinigung wird beendet** wird angezeigt, welche Arten von Arbeitsspuren bei Verwendung vertraulicher Daten bereinigt wurden.

Abbildung 80: Bereinigung abschließen

Zum Abschluss des Assistenten klicken Sie auf die Schaltfläche **Fertig**.

Vollständige Bereinigung einstellen

Damit Sie festlegen können, welche Daten beim Durchführen einer vollständigen Bereinigung sicher gelöscht werden sollen, gehen Sie wie folgt vor:

1 Wählen Sie im Menü **SafeDisk** den Punkt **Einstellungen**.

2 Öffnen Sie im Fenster **Einstellungen** die Registerkarte **Vollständige Bereinigung**.

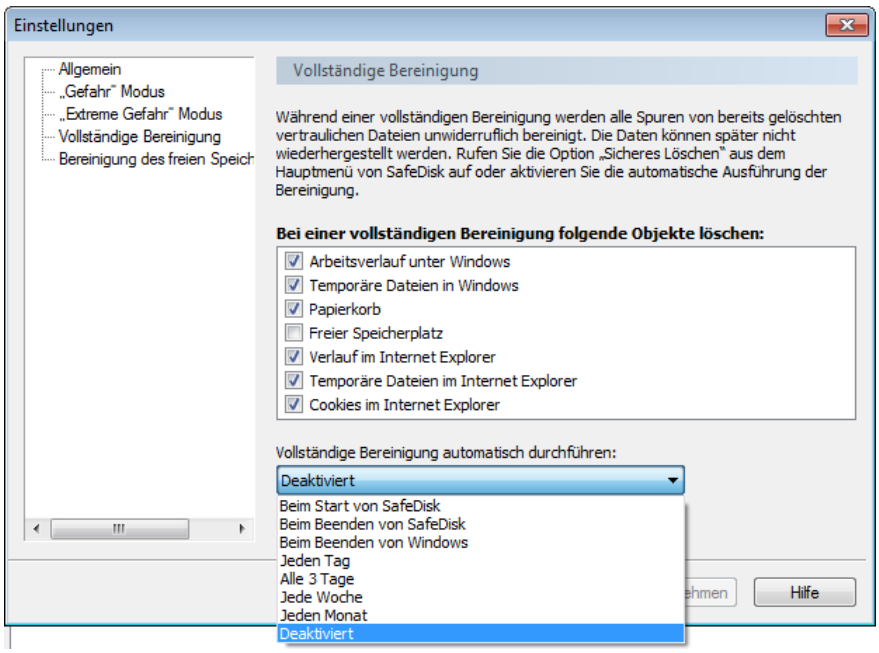
Einstellungen
Allgemein
„Gefahr" Modus
„Extreme Gefahr" Modus
Vollständige Bereinigung
Bereinigung des freien Speich
Vollständige Bereinigung
Während einer vollständigen Bereinigung werden alle Spuren von bereits gelöschten vertraulichen Dateien unwiderruflich bereinigt. Die Daten können später nicht wiederhergestellt werden. Rufen Sie die Option „Sicheres Löschen" aus dem Hauptmenü von SafeDisk auf oder aktivieren Sie die automatische Ausführung der Bereinigung.
Bei einer vollständigen Bereinigung folgende Objekte löschen:
Arbeitsverlauf unter Windows
Temporäre Dateien in Windows
Papierkorb
Freier Speicherplatz
Verlauf im Internet Explorer
Temporäre Dateien im Internet Explorer
Cookies im Internet Explorer
Vollständige Bereinigung automatisch durchführen:
Deaktiviert
Beim Start von SafeDisk
Beim Beenden von SafeDisk
Beim Beenden von Windows
Jeden Tag
Alle 3 Tage
Jede Woche
Jeden Monat
Deaktiviert
Hilfe

Abbildung 81: Bereiche für die vollständige Bereinigung definieren

3 Aktivieren Sie auf der Registerkarte **Vollständige Bereinigung** in der Liste **Bei einer vollständigen Bereinigung folgende Objekte löschen** die Kontrollkästchen neben den Objekten, die Sie standardmäßig bereinigen wollen.

4 Klicken Sie auf **Übernehmen** und dann auf **OK**.

Damit die vollständige Bereinigung automatisch durchgeführt wird:

1 Wählen Sie im Fenster **Einstellungen** auf der Registerkarte Vollständige Bereinigung (s. Abbildung auf Seite 157) in der Dropdownliste **Vollständige Bereinigung automatisch durchführen** einen der folgenden Einträge aus: **Beim Start von SafeDisk**, **Beim Beenden von SafeDisk**, **Beim Beenden von Windows**, **Jeden Tag**, **Alle 3 Tage**, **Jede Woche**, **Jeden Monat**, **Deaktiviert**.

2 Klicken Sie auf **Übernehmen** und dann auf **OK**.

Bereinigung über die Befehlszeile starten

ViPNet SafeDisk ermöglicht die Benutzung der Befehlszeile, um unterschiedliche Bereinigungsvorgänge zu starten. Dies kann in folgenden Fällen von Nutzen sein:

- Es müssen Spuren von Dateien eines bestimmten Typs bereinigt werden. Sie möchten zum Beispiel die Spuren aller `*.doc`-Dateien vernichten, da gerade die Dateien dieses Typs sensible Daten beinhalten.
- Es muss ein bestimmter Ordner auf der Festplatte bereinigt werden.
- Sie haben eine Batch-Datei (`*.bat`) erstellt und wollen darin die Bereinigungsbefehle von ViPNet SafeDisk verwenden. Zum Beispiel wollen Sie die Bereinigung mit Hilfe von ViPNet SafeDisk gemäß einem Zeitplan ohne weitere Benutzer-Interaktionen durchführen oder jedes Mal vor dem Ausschalten des Computers starten lassen.
- Sie haben ein Plug-In für Microsoft Word erstellt, um mit bestimmten Daten sicher arbeiten zu können. Die Sicherheitsanforderungen an dieses Plug-In erfordern die Vernichtung aller Arbeitsspuren nach der Handhabung vertraulicher Dokumente in Microsoft Word.
- Es müssen Bereinigungsbefehle von ViPNet SafeDisk ausgeführt werden, ohne dabei die graphische Benutzeroberfläche von ViPNet SafeDisk zu starten. Zum Beispiel wollen Sie es zu diesem Zeitpunkt vermeiden, andere Benutzer von ihren Aufgaben abzulenken.

Gehen Sie wie folgt vor, um Bereinigungsbefehle von ViPNet SafeDisk über eine Befehlszeile zu starten:

1. Starten Sie den Befehlszeileninterpreter.
2. Geben Sie den Pfad zur Utility-Datei `Clean.exe` ein. Standardmäßig befindet sich die Utility im Ordner `C:\Program Files\InfoTeCS\ViPNet SafeDisk\`.
3. Tippen Sie in der Befehlszeile die folgende Zeichenfolge ein: clean.exe – Leerzeichen – Schrägstrich (/) – benötigter Parameter. Die möglichen Parameter sind mitsamt der Beschreibung in der nachfolgenden Tabelle aufgelistet.

Tabelle 6. Befehle der Bereinigung in ViPNet SafeDisk

Befehle im Menü ViPNet SafeDisk (graphische Benutzeroberfläche)	**Befehle in der Befehlszeile (mit Parametern)**	**Ergebnisse**
Windows		
Freier Speicherplatz	`Clean.exe /f <Laufwerksbuchstabe>`	Der freie Speicherplatz auf dem ausgewählten Laufwerk wird bereinigt. Um freien Speicherplatz auf einem Laufwerk bereinigen zu können, müssen Sie über Schreibrechte für den Stammordner des Laufwerks verfügen.
Temporäre Dateien	`Clean.exe /t`	Temporäre Windows-Dateien werden sicher gelöscht.
Arbeitsverlauf	`Clean.exe /d`	Alle Verweise im Ordner **Zuletzt verwendete Dokumente** werden sicher gelöscht.
Papierkorb	`Clean.exe /r`	Papierkorb wird sicher bereinigt.
	`Clean.exe <Dateimaske>`	Dateien, die zur definierten Maske passen, werden aus dem angegebenen Ordner (standardmäßig aus dem aktuellen Ordner) entfernt. Beim Definieren der Maske gilt Folgendes: ? – ersetzt genau ein Symbol. * – ersetzt mehrere Symbole. Wenn Sie zum Beispiel die Maske *.doc definieren, werden alle Dateien mit der Erweiterung .doc entfernt.
	`Clean.exe <Ordnernahme>`	Ordnerinhalt wird gelöscht.
Internet Explorer		
Verlauf	Clean.exe /h	Browserverlauf im Internet Explorer wird bereinigt.
Temporäre Dateien	`Clean.exe /i`	Temporäre Internetdateien werden gelöscht.
Cookies	`Clean.exe /c`	Cookies werden gelöscht.

Tipp. Sie können die Utility Clean.exe mit mehreren Parametern gleichzeitig starten. Zum Beispiel: `Clean.exe /c /h /i /t /r /d /fc c:\folder1\*.* c:\folder2`.

11

Suche und Beseitigung von Störungen

Logdatei ansehen 163

Typische Problemfälle 164

Logdatei ansehen

Zum Anzeigen der Logdatei von ViPNet SafeDisk:

1. Öffnen Sie den Programmordner. Standardmäßig wird ViPNet SafeDisk in den folgenden Ordner installiert:
   - `C:\Users\User\AppData\Roaming\InfoTeCS\SafeDisk`, für Betriebssysteme Windows Vista und höher oder Windows Server 2008;
   - `C:\Documents and Settings\User\Application Data\Infotecs\Safedisk\`, für Betriebsysteme Windows XP oder Windows Server 2003.
2. Öffnen Sie die Datei „SDEvents.log“. Die Datei enthält Informationen über folgende Ereignisse:
   - Benutzeranmeldung im Programm.
   - Benutzerabmeldung im Programm.
   - Aktivierung des „Gefahr“ Modus.
   - Aktivierung des „Extreme Gefahr“-Modus.
   - Alle Vorgänge, die sich auf Container beziehen (unter Angabe des Containernamens): Erstellung eines neuen Containers, Einbindung des Containers, Trennen des Containers, Löschen des Containers, Container-Import, Container-Export, Änderung der Container-Eigenschaften.

Für jedes Ereignis werden folgende Daten registriert:

- Ereignisdatum und –zeit.
- Ereignisstatus: erfolgreicher Abschluss oder Abbruch.

Typische Problemfälle

Container ist nicht verfügbar

Wenn beim Versuch, einen neuen Container einzubinden, die Meldung eingeblendet wird, dass der Container nicht verfügbar ist:

1. Öffnen Sie den Ordner **Arbeitsplatz**.
2. Drücken Sie die Taste **F5**, um den Ordner zu aktualisieren. Ein neues lokales Laufwerk wird angezeigt.

Formatieren Sie den Container, bevor Sie ihn verwenden.

Laufwerk kann nicht formatiert werden

Wenn das Programm ViPNet SafeDisk auf einem Computer mit dem Betriebssystem Windows installiert ist, und Sie über keine Administratorrechte in diesem System verfügen, dann können Sie das Laufwerk des Containers nicht formatieren. Um dieses Problem zu lösen, müssen Sie entweder Administratorrechte erlangen oder Ihren Systemadministrator bitten, den Container für Sie zu erstellen und auf Ihrem Computer zu importieren.

Container-Datei wurde nicht gefunden

Wenn beim Starten des Programms ein früher erstellter Container nicht gefunden werden kann, wird dieser Container im ViPNet SafeDisk-Programmfenster mit dem Symbol gezeichnet.

Wenn sich die Datei Ihres Containers auf einem Netzlaufwerk befindet und der Container sich nicht in ViPNet SafeDisk einbinden lässt:

- Überprüfen Sie, ob der Containername geändert wurde.
- Überprüfen Sie, ob der Pfad zur Container-Datei geändert wurde.
- Wenn sich die Datei Ihres Containers auf einem Netzlaufwerk befindet, überprüfen Sie den Status der Netzwerkverbindung.

- Wenn sich die Datei Ihres Containers auf einem Netzlaufwerk befindet, überprüfen Sie, ob sich der Name der Container-Datei geändert hat.

Achtung! Wenn Sie möchten, dass Ihr Container, der sich auf einem Netzlaufwerk befindet, als ein eigenes Netzlaufwerk freigegeben wird, dann sollte der Name der Container-Datei nicht nachträglich geändert werden.

Beim Versuch, einen nicht auffindbaren Container einzubinden, wird das Fenster **Container nicht gefunden** eingeblendet. Um den Zugang zu in diesem Container enthaltenen Daten wiederherzustellen, geben Sie den neuen Pfad zur Container-Datei an.

CONTAINER1CAA nicht gefunden
Container wurde nicht gefunden. Eventuell wurde der Container auf einem tragbaren Datenträger gespeichert, der momentan nicht angeschlossen ist, oder auf der Festplatte und wurde an einen anderen Ort verschoben.
Geben Sie den Pfad zu dem Container ein:
ED FOLDERS\D\!_WORK\CONTAINER\CONTAINER1CAA.SDC
...
OK
Abbrechen

Abbildung 82: Container nicht gefunden

Verbindung zum Container ging verloren

Wenn zu einem Container, der sich auf einem Netzlaufwerk oder einem mobilen Datenträger befindet, keine Verbindung mehr besteht:

1. Trennen Sie den Container.
2. Richten Sie die Verbindung zum Netzlaufwerk wieder ein (oder warten Sie ab, bis die Verbindung wiederhergestellt wird).
3. Binden Sie den Container erneut ein (s. Einen früher erstellen Container einbinden auf Seite 77).

Container kann nicht eingebunden werden

Wenn Sie einen Container nicht einbinden können:

- Vergewissern Sie sich dass der Container nicht von einem anderen Benutzer eingebunden ist. Dies ist möglich wenn das Laufwerk des Containers freigegeben wurde.

  Ein gleichzeitiger Zugriff mehrerer Benutzer auf einen Container ist nicht möglich.

- Container-Datei wurde nicht gefunden (auf Seite 164).

Das Komprimierungs- oder das Verschlüsselungsattribut der Container-Datei ist gesetzt

In der aktuellen Programmversion kann als Container keine Datei verwendet werden, bei welcher das Komprimierungs- oder das Verschlüsselungsattribut gesetzt ist. Beim Versuch, einen solchen Container einzubinden, wird eine Meldung über die Unmöglichkeit der Einbindung eingeblendet.

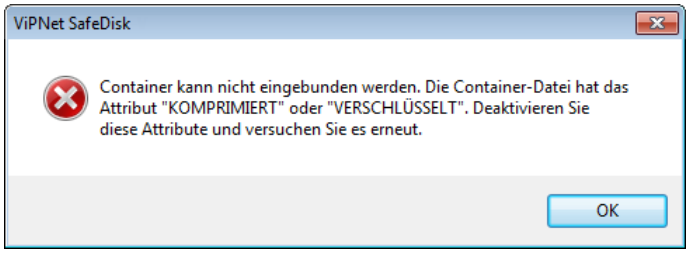
ViPNet SafeDisk
Container kann nicht eingebunden werden. Die Container-Datei hat das Attribut "KOMPRIMIERT" oder "VERSCHLÜSSELT". Deaktivieren Sie diese Attribute und versuchen Sie es erneut.
OK

Abbildung 83: Container kann nicht eingebunden werden

Das Komprimierungs- oder Verschlüsselungsattribut kann beim Erstellen der Container-Datei automatisch gesetzt worden sein, falls das Komprimierungsattribut sowohl für das Laufwerk, auf dem der Container angelegt wird, als auch für alle untergeordneten Dateien und Ordner auf diesem Laufwerk gesetzt wurde.

Zum Zurücksetzen des Komprimierungs- oder des Verschlüsselungsattributs:

1. Klicken Sie mit der rechten Maustaste auf den Container-Dateinamen und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**.
2. Klicken Sie im Fenster der Datei-Eigenschaften in der Registerkarte **Allgemein** auf die Schaltfläche **Erweitert**.
3. Deaktivieren Sie im Fenster **Erweiterte Attribute** in Gruppe **Komprimierungs- und Verschlüsselungsattribute** die entsprechenden Kontrollkästchen.

Container mit Zugriffstyp „Authentisierungsgerät" konnte nicht erstellt werden

Wenn beim Versuch, einen neuen Container unter Verwendung des Zugriffstyps **Authentisierungsgerät** zu erstellen, vom Programm die Meldung ausgegeben wird, dass der Container nicht erstellt werden kann:

1. Stellen Sie sicher, dass das angeschlossene externe Gerät vom Programm ViPNet SafeDisk unterstützt wird. Eine Liste aller unterstützten Geräte finden Sie im Kapitel Externe Datenträger (auf Seite 171).
2. Stellen Sie sicher, dass auf dem externen Gerät alle erforderlichen Treiber oder Programme für die Arbeit mit Schlüsseln installiert sind. Die erforderlichen Voraussetzungen für die Arbeit mit Authentisierungsgeräten sind im Kapitel Externe Datenträger (auf Seite 171).
3. Überprüfen Sie, ob die Initialisierung des Authentisierungsgeräts korrekt durchgeführt wird. Wenn zum Beispiel bei der Initialisierung des Geräts festgestellt wurde, dass beim nächsten Verbinden die PIN geändert werden sollte, und Sie bislang aber keinen PIN-Wechsel durchgeführt haben, dann kann dieses Gerät nicht zum Speichern der Container-Schutzschlüssel verwendet werden.
4. Löschen Sie alle Daten aus dem privaten Speicher des Authentisierungsgeräts. Führen Sie dazu die Initialisierung des Authentisierungsgeräts durch. Eine Anleitung zur Durchführung der Initialisierung finden Sie im Handbuch des verwendeten Geräts.
5. Versuchen Sie, ein anderes Gerät mit einem größeren Volumen an privatem Speicher zu benutzen.

Versionsgeschichte

In dieser Anwendung werden die wichtigsten Änderungen in den vorherigen Versionen von ViPNet SafeDisk beschrieben.

Version 3.2.2

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.2.2 geboten.

- **Französische Lokalisierung**

  Eine vollständige Lokalisierung des Produkts in französischer Sprache wurde durchgeführt. Lokalisiert wurden die Benutzeroberfläche, die Hilfe und die Dokumentation.

- **Verbesserte Dokumentation und Online-Hilfe**

  Dokumentation und Online-Hilfe wurden komplett überarbeitet, ihre Qualität wurde verbessert. Bei der Überarbeitung der Dokumentation wurde spezielle Aufmerksamkeit einem Szenario-basierten Ansatz gewidmet.

Version 3.2.1

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.2.1 geboten.

- **Möglichkeit zur Eingabe einer alphanumerischen PIN**

Es besteht die Möglichkeit, bei Verwendung externer Geräte nicht nur numerische, sondern auch alphanumerische PINs anzugeben.

Version 3.2.0

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.2.0 geboten.

- **Unterstützung von 64-Bit-Betriebssystemen**

  Folgende Betriebssysteme werden unterstützt: Windows XP Pro (64-Bit), Windows Vista (64-Bit), Windows Server 2008 (64-Bit), Windows 7 (32/64-Bit).

Version 3.1.1

In Version 3.1.1 wurden kritische Fehler beseitigt, die in Version 3.1.0 entdeckt wurden.

Version 3.1.0

In diesem Abschnitt wird eine kurze Übersicht der Änderungen und neuen Möglichkeiten der Version 3.1.0 geboten.

- **Möglichkeit der Verwendung sowohl der registrierten als auch der unregistrierten Version**

  Nun kann das Programm sowohl als Free Edition, bei welcher keine Registrierung erforderlich ist, die jedoch einigen funktionellen Einschränkungen unterliegt, als auch in der Vollversion, bei welcher eine Registrierung notwendig ist, eingesetzt werden. Es gibt keine Testversion mehr.

  Der Einsatz der unregistrierten Version 3.1.0 sieht folgende Einschränkungen vor:

  - maximale Anzahl der Benutzer – 1,
  - maximale Anzahl der Container – 1,
  - maximale Containergröße – 100 MB.

  Die nicht registrierte Version wird kostenlos zur Verfügung gestellt und hat keine Beschränkung der Gültigkeitsdauer. Bei einer Registrierung fallen alle aufgezählten Einschränkungen weg.

- **Die Befehle zum sicheren Löschen von Daten sind im Hauptprogrammfenster verfügbar**

Befehle zum sicheren Löschen von Informationen, welche in den vorhergehenden Versionen nur über die Kommandozeile ausgeführt werden konnten, sind jetzt im Hauptfenster des Programms im Menü **Sicheres Löschen** verfügbar. Die Konfiguration der Parameter für das sichere Löschen erfolgt mit Hilfe eines Assistenten.

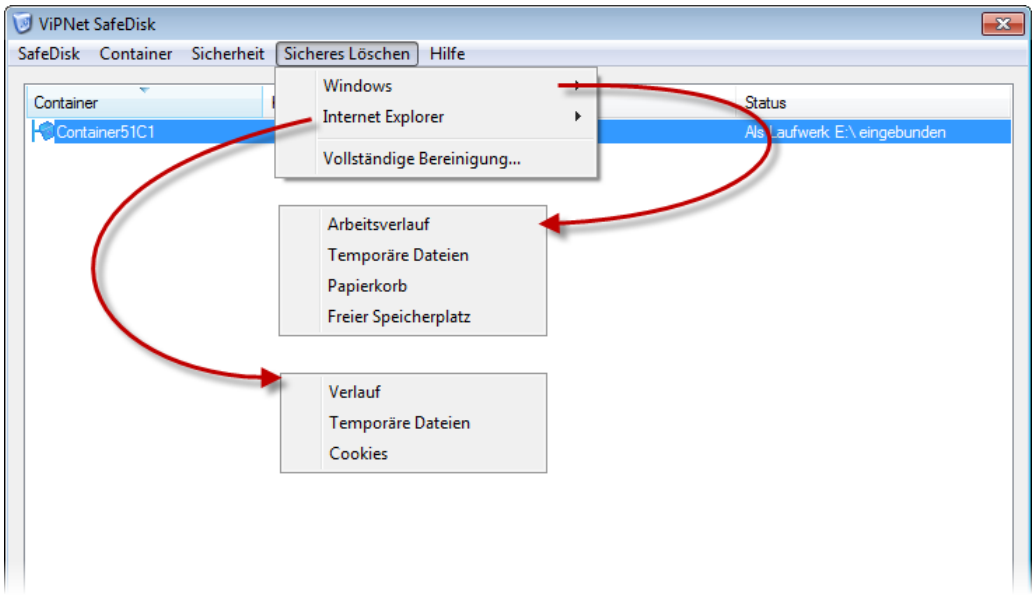

Abbildung 84: Befehle für das sichere Löschen von Daten

Es besteht die Möglichkeit, Befehle zum sicheren Löschen von Dateien auf der Festplatte nach Eintritt bestimmter Ereignisse oder in bestimmten Zeitabständen auszuführen.

- **Verwendung von ACOS2-8k Smartcards als externe Authentisierungsgeräte**

  In die Liste unterstützter Geräte, mit deren Hilfe der Zugang zu den Benutzercontainern geschützt werden kann, wurden die ACOS2-8k Smartcards aufgenommen. Die Kommunikation mit den ACOS2-8k Smartcards erfolgt über die Standardschnittstelle PC/SC.

- **Anzeige des Verlaufs der Container-Formatierung**

  Der Benutzer wird über den Fortschritt der Containerformatierung informiert, falls der Vorgang eine längere Zeit in Anspruch nimmt.

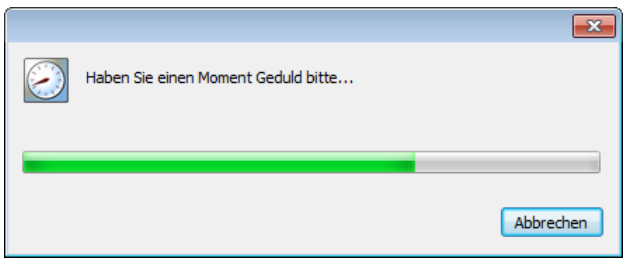

Abbildung 85: Der Verlauf der Containerformatierung

B

Externe Datenträger

Die ViPNet-Software ermöglicht die Verwendung verschiedener externer Datenträger (Geräte) zum Speichern und Auslesen von Informationen (Passwörter, Schlüssel u.a.).

Achtung! Auf einem Datenträger können nicht mehrere Schlüsseldistributionen gespeichert werden. Vor dem Speichern der Schlüsseldistributionen vergewissern Sie sich bitte, dass der Datenträger formatiert ist. Auf einem Datenträger können mehrere Signaturschlüssel gespeichert werden.

In der unten aufgeführten Tabelle sind alle, mit ViPNet Software kompatiblen, Geräte und Schlüssel aufgelistet. Die Tabelle enthält folgende Angaben:

- In der Spalte **Gerätetyp** sind alle Lesegerättypen aufgelistet, die mit der ViPNet Software kompatibel sind.
- In der Spalte **Schlüsselart** werden die Typen der Schlüssel für das jeweilige Lesegerät aufgeführt.
- In der Spalte **Anwendungsbedingungen** werden die Mindestanforderungen für jeden Schlüssel angegeben.
- In der Spalte Unterstützung von PKCS#11 wird angegeben, ob dieser Standard unterstützt wird.

Hinweis. PKCS#11 Standard (bekannt auch als Cryptoki) gehört zur Gruppe der PKCS Standards (Public Key Cryptography Standards – Verschlüsselungsstandards für öffentliche Schlüssel), welche von der Firma RSA Laboratories entwickelt wurde. Der Standard beschreibt eine betriebssystemunabhängige API-Benutzeroberfläche für die

Arbeit mit kryptografischen Authentisierungsgeräten.

Gerätetyp	Schlüsselart	Anwendungsbedingungen	Unterstützung von PKCS#11
eToken Aladdin	**eToken PRO** (persönlicher elektronischer Schlüssel Token PRO (Java), eToken PRO, SmartCard eToken PRO (Java), eToken PRO vom Hersteller Aladdin).	• Auf dem Netzwerkknoten muss die Software PKI Client 5.1 oder höher installiert sein. • Kompatible Betriebssysteme: Windows XP SP3 (32 Bit), Server 2003 SP2 (32 Bit), Vista SP2 (32/64 Bit), Windows 7 (32/64 Bit), Server 2008 (32/64 Bit), Server 2008 R2. • **Hinweis:** eToken PRO SmartCard kann mit jedem PC/SC-kompatiblen Smart Card Reader benutzt werden.	Ja
iButton	**iButton (Dallas)** (elektronischer Schlüssel iButton DS1993, DS1994, DS1995 und DS1996).	• Das Lesegerät muss an den Computer angeschlossen werden. • Auf dem Computer muss die Software zur Datenübertragung mit iButton, 1-Wire Drivers Version 3.6.2 installiert sein. • Kompatible Betriebssysteme: Windows XP SP3 (32 Bit), Server 2003 (32 Bit), Vista SP2 (32 Bit), Server 2008 (32 Bit), Windows 7 (32 Bit).	Nein
Smartcard Athena	Karten mit dem Speichertyp I2C (ASE M4), synchrone Karten mit dem Bustyp 2/3 und geschütztem Speicher nach ISO7816-3 (ASE MP42).	• Das Auslesen und Eintragen der Daten auf Smartcard erfolgt durch den CardReader ASEDrive III PRO-S des Herstellers Athena. • Die Treiber der Version 2.6 sollen auf dem PC installiert werden. • Kompatible Betriebssysteme: Windows XP SP3 (32 Bit), Server 2003 (32 Bit), Vista SP2 (32/64 Bit).	Nein
Siemens CardOS (wird nicht von ViPNet CSP unterstützt)	**SmartCard Siemens** (CardOS/M4.01a, CardOS V4.3B, CardOS V4.2B, CardOS V4.2B DI, CardOS V4.2C, CardOS V4.4).	• Auf dem Computer muss die Software Siemens CardOS API V5.0 oder höher installiert werden. • Kompatible Betriebssysteme: Windows XP SP3 (32 Bit), Server 2003 EE SP2 (32 Bit), Vista SP2 (32/64 Bit), Server 2008 SP2 (32/64 Bit), Windows 7 (32/64 Bit).	Ja

C

Regionaleinstellungen

Zur korrekten Darstellung des deutschen Interfaces von ViPNet Client im Betriebssystem Microsoft Windows XP/Vista/Windows 7 mit englischer Lokalisierung sollte die Unterstützungsfunktion von Umlauten und „ß“ aktiviert werden. Das gilt besonders für Programme, die keinen Unicode-Standard unterstützen. Es wird empfohlen, diese Einstellung bereits vor der Programminstallation durchzuführen.

Achtung! Diese Parameter sollten auch dann eingestellt werden, wenn ein deutsches MUI (Multilanguage User Interface) installiert wurde. Das bedeutet, dass der Kern des Betriebssystems Englisch ist und die deutsche Sprache für das Interface und die Help-Dateien später installiert wurde. In diesem Fall sind die Regionaleinstellungen Englisch und sollten geändert werden.

So konfigurieren Sie die Spracheinstellungen für Windows XP:

1. Wählen Sie **Systemsteuerung** im Menü **Start** (**Control Panel**) aus.
2. Klicken Sie auf **Datums-, Zeit-, Sprach- und Regionaleinstellungen** (**Regional and Language Options**) und dann auf **Regions- und Sprachoptionen**.
3. Gehen Sie zu der Registerkarte **Erweitert** (**Advanced**) im Fenster **Regions- und Sprachoptionen** (**Regional and Language Options**)
4. Wählen Sie **Deutsch** (**German**) aus.
5. Aktivieren Sie das Kontrollkästchen **Alle Einstellungen auf das Benutzerkonto und Standardbenutzerprofil anwenden** (**Apply all settings to the current user account and to the default user profile**).

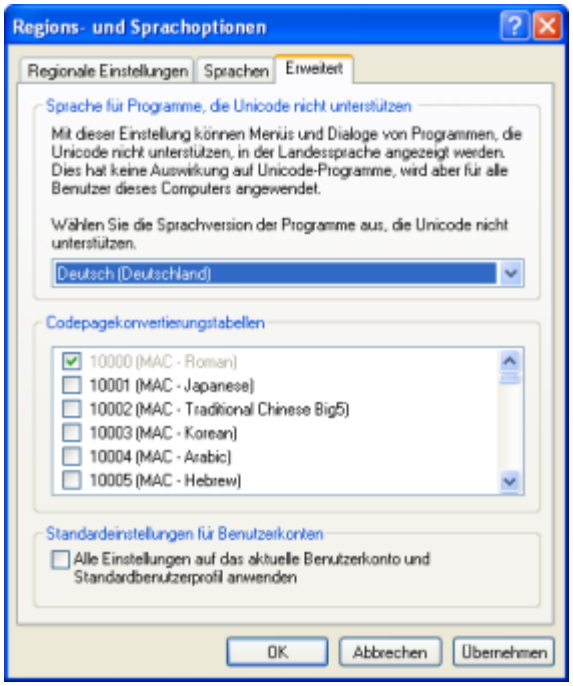
Regions- und Sprachoptionen
Regionale Einstellungen
Sprachen
Erweitert
Sprache für Programme, die Unicode nicht unterstützen
Mit dieser Einstellung können Menüs und Dialoge von Programmen, die Unicode nicht unterstützen, in der Landessprache angezeigt werden. Dies hat keine Auswirkung auf Unicode-Programme, wird aber für alle Benutzer dieses Computers angewendet.
Wählen Sie die Sprachversion der Programme aus, die Unicode nicht unterstützen.
Deutsch (Deutschland)
Codepagekonvertierungstabellen
10000 (MAC - Roman)
10001 (MAC - Japanese)
10002 (MAC - Traditional Chinese Big5)
10003 (MAC - Korean)
10004 (MAC - Arabic)
10005 (MAC - Hebrew)
Standardeinstellungen für Benutzerkonten
Alle Einstellungen auf das aktuelle Benutzerkonto und Standardbenutzerprofil anwenden
OK
Abbrechen
Übernehmen

Abbildung 86: Sprachauswahl für Programme, die Umlaute und „ß“ nicht unterstützen

6 Klicken Sie auf **OK**. Möglicherweise muss der Computer neu gestartet werden.

Auf diese Weise erreichen Sie die korrekte Darstellung der Umlaute und „ß“ für Windows Vista/Windows 7:

1 Wählen Sie Systemsteuerung im Menü **Start** (**Control Panel**) -> **Zeit, Sprache und Region** (**Clock, Language, and Region**) -> **Region und Sprache** (**Region and Language**) aus.

2 Klicken Sie auf die Registerkarte **Verwaltung** (**Administrative**) im Fenster **Region und Sprache** (**Region and Language**).

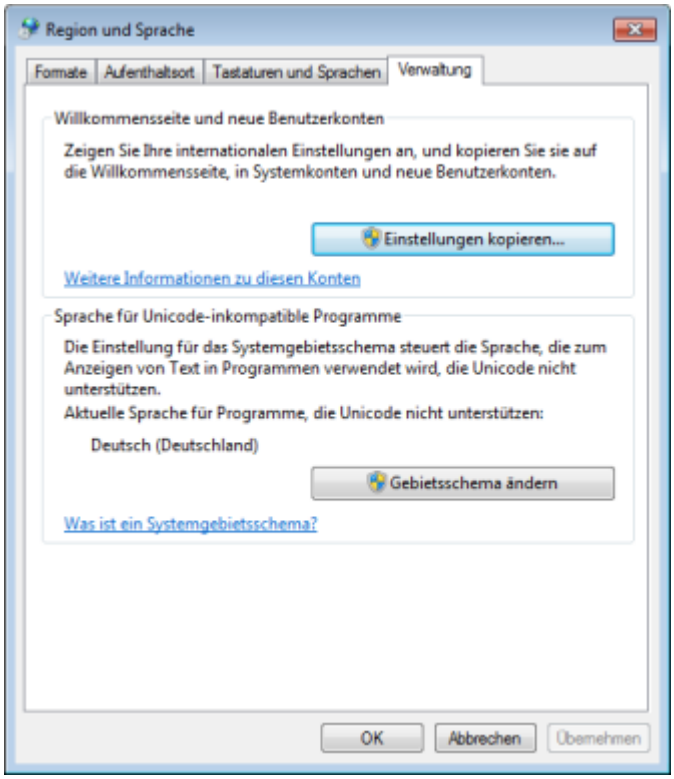
Region und Sprache
Formate
Aufenthaltsort
Tastaturen und Sprachen
Verwaltung
Willkommensseite und neue Benutzerkonten
Zeigen Sie Ihre internationalen Einstellungen an, und kopieren Sie sie auf die Willkommensseite, in Systemkonten und neue Benutzerkonten.
Einstellungen kopieren...
Weitere Informationen zu diesen Konten
Sprache für Unicode-inkompatible Programme
Die Einstellung für das Systemgebietsschema steuert die Sprache, die zum Anzeigen von Text in Programmen verwendet wird, die Unicode nicht unterstützen.
Aktuelle Sprache für Programme, die Unicode nicht unterstützen:
Deutsch (Deutschland)
Gebietsschema ändern
Was ist ein Systemgebietsschema?
OK
Abbrechen
Übernehmen

Abbildung 87: Erweiterte Spracheinstellungen

3 Klicken Sie auf **Gebietsschema ändern** (**Change system locale**) in der Registerkarte **Verwaltung** (**Administrative**).

4 Wählen Sie **Deutsch (Deutschland)** im neu geöffneten Fenster in der Liste **Aktuelles Gebietsschema** aus und klicken auf **OK**.

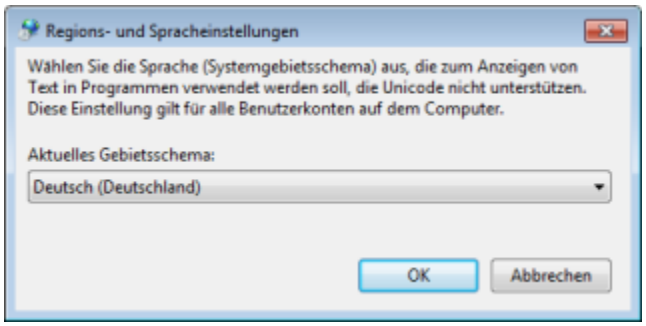
Regions- und Spracheinstellungen
Wählen Sie die Sprache (Systemgebietsschema) aus, die zum Anzeigen von Text in Programmen verwendet werden soll, die Unicode nicht unterstützen.
Diese Einstellung gilt für alle Benutzerkonten auf dem Computer.
Aktuelles Gebietsschema:
Deutsch (Deutschland)
OK
Abbrechen

Abbildung 88: Auswahl der Systemsprache

5 Klicken Sie auf die Schaltfläche **Einstellungen kopieren** (**Copy settings**) in der Registerkarte **Verwaltung** (**Administrative**).

6 Aktivieren Sie das Kontrollkästchen **Willkommensseite und Benutzerkonten** (**Welcome screen and system accounts**) im neu geöffneten Fenster und klicken auf **OK**.

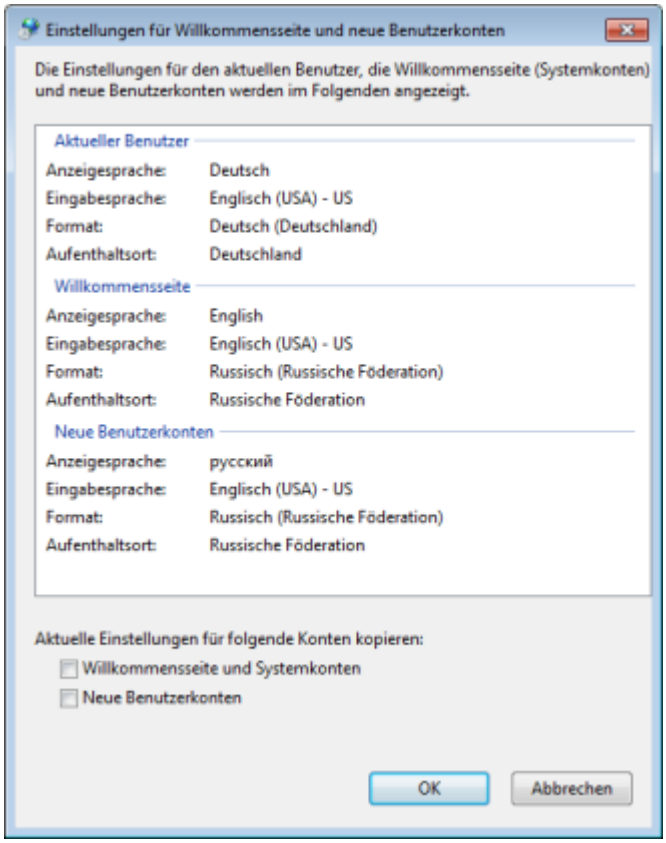

Abbildung 89: Kopieren der Parameter

Um weitere Probleme mit der Zeichencodierung auf einigen Systemen zu vermeiden, nehmen Sie die folgenden Einstellungen vor:

1 Gehen Sie zur Registerkarte **Formate** (**Formats**) des Fensters **Region und Sprache** (**Region and Language**) und wählen Sie **Deutsch (Deutschland)** in der Liste **Format** aus.

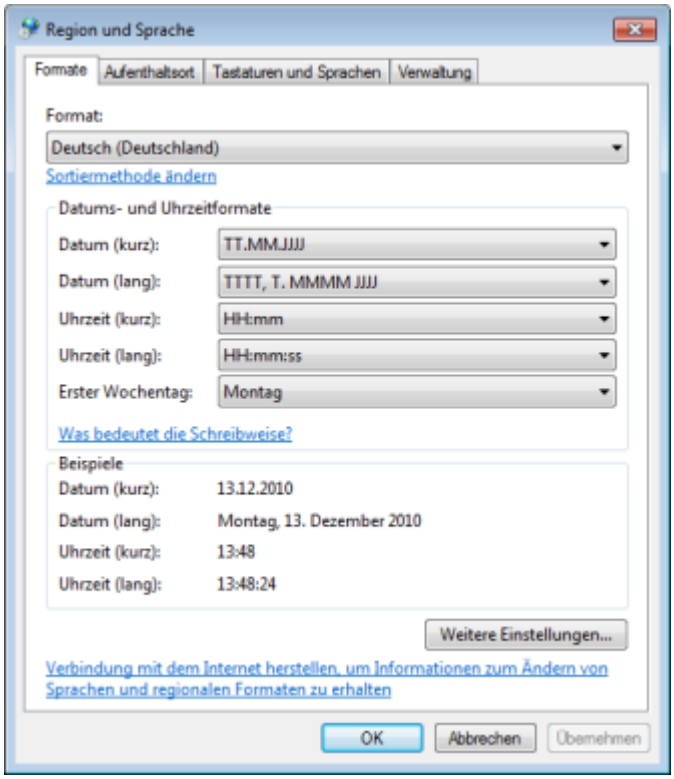

Abbildung 90: Einstellung von Formaten

2 Gehen Sie zur Registerkarte **Aufenthaltsort** (**Location**) des Fensters **Region und Sprache** (**Region and Language**) und wählen Sie **Deutschland** in der Liste **Aktueller Aufenthaltsort** (**Current location**) aus.

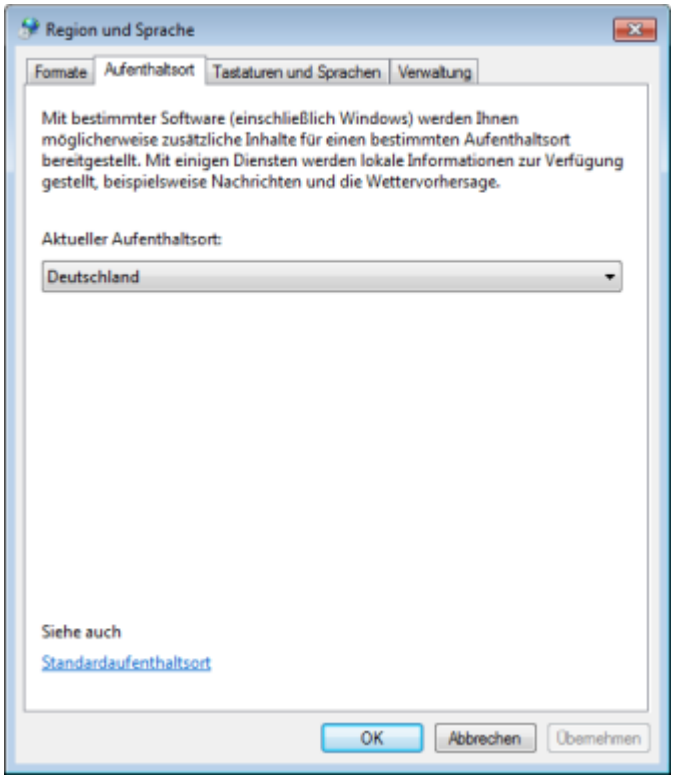

Abbildung 91: Auswahl des aktuellen Aufenthaltsortes

Glossar

C

Container

Siehe Container-Datei (auf Seite 179).

Container-Datei

Eine Datei, welche die geschützten Daten beinhaltet. Diese Datei wird als ein Laufwerk unter Windows angezeigt. Sie können mit ihr wie mit einem Laufwerk arbeiten und dort Dateien speichern, kopieren, einfügen, verschieben, löschen usw.

Eine Containerdatei hat die Dateierweiterung *.sdc und ist standardmäßig ausgeblendet. Um diese Datei anzusehen wählen Sie in der Windows-Explorer Menüleiste unter **Extras** den Menüpunkt **Ordner- und Suchoptionen** und auf der Registerkarte **Ansicht** deaktivieren Sie die Option **Geschützte Dateien ausblenden (empfohlen)**.

D

Digitales Roulette

Eingebaute Komponente der ViPNet-Software, die es ermöglicht, den Zufallszahlengenerator anhand von Benutzeraktionen zu initialisieren.

E

Exportdatei des Containers

Diese Datei wird beim Containerexport erstellt. Sie beinhaltet die exportierte Containerdatei und die Sicherungskopie der Containerschlüssel.

Sie können einen Container exportieren, wenn Sie eine vollständige Sicherungskopie aller Daten erstellen wollen, die im Container enthalten sind, oder wenn Sie einem anderen Benutzer den Zugriff auf die geschützten Daten ermöglichen wollen.

Die Exportdatei des Containers hat die Erweiterung `*.sdx`.

Siehe: Sicherungskopie der Containerschlüssel (auf Seite 180).

F

Fiktiver Benutzer

Ein fiktives Benutzerkonto in ViPNet SafeDisk, das Sie erstellen können, um die Arbeit mit geschützten Daten zu imitieren, während Sie sich im Sichtfeld unberechtigter Dritter befinden. Es ist empfehlenswert, ein fiktives Benutzerkonto im Voraus anzulegen.

M

Modus „Extreme Gefahr“

Spezialmodus von ViPNet Safe Disk, der es ermöglicht, alle Daten in den Containern unverzüglich zu löschen, wenn beim Näherkommen unberechtigter Übeltäter keine andere Wahl mehr bleibt.

Siehe: Modus „Gefahr“ (auf Seite 180).

Modus „Gefahr“

In diesem Modus können alle Container sofort getrennt werden.

Siehe auch: Modus „Extreme Gefahr“ (auf Seite 180).

S

Sicherungskopie der Containerschlüssel

Spezielle Datei, die eine Kopie der Schlüssel enthält, mit deren Hilfe der Container geschützt wird. Wenn die Schlüssel-Datei für den Zugang zum Container beschädigt ist, oder Sie aus

anderen Gründen den Zugang zum Container nicht erhalten, verwenden Sie zum Wiederherstellen des Containerzugangs die Sicherungskopie der Containerschlüssel. Sie können die Sicherungskopie auch verwenden, um jemand anderem Zugang auf Ihren Container zu gewähren.

Die Datei mit der Sicherungskopie der Containerschlüssel hat die Erweiterung `*.sde`.

Z

Zugriffstyp auf den Container

ViPNet SafeDisk ermöglicht es, beim Zugriff auf den Container eine der folgenden Zugriffsarten auszuwählen: **Passwort** (für den Zugriff auf den Container reicht es, ein Passwort bei der Anmeldung in ViPNet SafeDisk anzugeben); **Schlüssel-Datei** (für den Zugriff auf den Container wird eine Schlüssel-Datei benötigt); **Authentisierungsgerät** (für den Zugriff auf den Container muss ein Authentisierungsgerät an den Rechner angeschlossen werden).

Index

A
Abgrenzung des Containerzugangs • 81, 122
Arbeit unter Kontrolle der Attentäter • 134

B
Benutzerpasswort definieren • 40, 120
Bereinigung über die Befehlszeile starten • 147
Bereinigung von Datenspuren
Reihenfolge der Schritte • 60

C
Container einbinden • 26, 135
Container einbinden, der durch eine Authentisierungsgeräti geschützt ist • 78
Container einbinden, der durch eine Schlüssel-Datei geschützt ist • 78
Container erstellen • 60, 106, 135
Container exportieren • 60, 69, 110, 111, 116, 132
Container löschen • 61
Container mit Hilfe der Sicherungskopie der Containerschlüssel importieren • 110, 115
Container mit Zugriffstyp • 66
Container-Datei • 67, 179
Container-Datei verschieben • 85
Containereigenschaften ansehen und ändern • 24
Containerschlüssel aktualisieren • 86, 124
Containerzugang für einen oder mehrere Benutzer auf demselben oder auf unterschiedlichen Computern bereitstellen • 89, 121
Cookies bereinigen • 148

D
Dateien sicher löschen • 151
Datenschutz mit Hilfe von ViPNet SafeDisk • 36
Datenspuren im Internet Explorer bereinigen • 146, 148
Datenspuren in Windows bereinigen • 146
Digitales Roulette • 38

E
Eigenes Passwort definieren • 36, 37
Einen früher erstellen Container einbinden • 125, 135, 165
Einschränkungen der kostenlosen Version • 23, 42
Exportdatei des Containers • 99
Externe Datenträger • 12, 15, 65, 87, 167

F
Freien Speicherplatz auf Laufwerken bereinigen • 148, 151

G
Geschützte Daten exportieren und importieren • 132

K
Konvertierung des Containers • 26

L
Liste zuletzt verwendeter Dateien löschen • 148

M
Modus • 180

N
Netzwerkzugang auf einen Container für die anderen Benutzer deaktivieren • 129, 130
Netzwerkzugang auf einen Container für mehrere Benutzer ermöglichen • 121, 130

P
Papierkorb bereinigen • 148
Parameter von ViPNet SafeDisk einstellen • 30, 149

R
Regionaleinstellungen • 23
Registrierung starten • 54
Registrierung von ViPNet SafeDisk • 16, 23, 61
Registrierungsanfrage per Registrierungsdatei • 45, 57
Registrierungsanfrage per Telefon • 45
Registrierungsanfrage über das Internet • 45, 48
Registrierungsanfrage via E-Mail • 45
Registrierungscode anfordern • 43, 44, 56
Registrierungsdaten speichern • 42, 48, 51, 55

S
Seriennummer anfordern • 43, 46, 57
Sicheres Löschen ungeschützter Dateien • 148
Sicherungskopie der Containerschlüssel • 70, 180
Sicherungskopie der Containerschlüssel erstellen • 60, 64, 67, 76, 105, 123, 131, 132
Sicherungskopie der Konfiguration erstellen • 40
Spurenbeseitigung bei der Arbeit mit privaten Daten • 33

T
Tastenkombinationen (Hotkeys) für den • 134
Temporäre Dateien löschen • 148
Temporäre Internetdateien löschen • 148

V
Vertrauliche Daten vernichten. • 33, 131, 134
ViPNet SafeDisk beenden • 33, 81
ViPNet SafeDisk registrieren • 43, 49, 52, 53
ViPNet SafeDisk starten • 26, 36, 81, 119, 135
ViPNet SafeDisk zum ersten Mal starten • 29, 61
Vollständige Bereinigung • 147
Vorbereitung auf die Arbeit unter Kontrolle der Attentäter • 134
Vorbereitung für den Einsatz in einer unsicheren Umgebung
  Vorgehensweise • 60
Vorgehensweise bei der Registrierung per Registrierungsdatei • 42, 52
Vorgehensweise beim Datenschutz • 130

W
Wenn sich die Konfiguration Ihres Rechners geändert hat • 42
Wiederherstellen des Zugriffs auf die geschützten Daten • 82, 100, 103

Z
Zufälliges Passwort generieren • 36, 37
Zugang zu allen Containern durch Wiederherstellung der Konfiguration wieder herstellen • 60, 110
Zugang zu geschützten Daten sofort blockieren. • 84, 131, 134
Zugriff auf die geschützten Daten verwalten. Neuen Benutzer registrieren • 29, 103, 135